COMMUNICATIONS
SECURITY
ESTABLISHMENT
COMMISSIONER

Annual Report

2008-2009

Canada

Office of the Communications Security
Establishment Commissioner
P.O. Box 1984, Station "B"
Ottawa, Ontario
K1P 5R5

Tel.: (613) 992-3044
Fax: (613) 992-4096
Website: www.ocsec-bcest.gc.ca

© Minister of Public Works and
Government Services Canada 2009
ISBN 978-0-662-06812-9
Cat. No. D95-2009

Cover photos: Malak

Communications Security
Establishment Commissioner

The Honourable Charles D. Gonthier, C.C., Q.C.

CANADA

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Charles D. Gonthier, C.C., c.r.

June 2009

Minister of National Defence
MGen G.R. Pearkes Building, 13th Floor
101 Colonel By Drive, North Tower
Ottawa, Ontario
K1A 0K2

Dear Sir:

Pursuant to subsection 273.63(3) of the *National Defence Act*, I am pleased to submit to you my 2008–2009 annual report on my activities and findings, for tabling in Parliament.

Yours sincerely,

Charles Gonthier

Charles D. Gonthier

P.O. Box/C.P. 1984, Station "B"/Succursale «B»
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax: (613) 992-4096

TABLE OF CONTENTS

Introduction /1

The Review Environment /2
- Proposed amendments to the *National Defence Act* /2
  - Ensuring the integrity of CSEC's activities and the review process /2
  - Applying a qualified opinion /3
  - Observations of the Auditor General /3
- Review cooperation /3
- Parliamentary committee involvement /4

The Year in Review /5
- Safeguarding privacy: Regular review of identity disclosures /5
- Briefings from CSEC /6
- More effective review through annual roundtables /6
- Strengthening lawful compliance /6
- A comprehensive review process /7

Methodology /8
- Identifying risks to lawfulness and privacy /8
- Attributes of a good review /8
  - Developing review findings and recommendations /9

2008–2009 Review Highlights /10
- Reviews of foreign intelligence activities under ministerial authorizations — Common elements /10
- Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 1) /11
- Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 2) /12
- Review of CSEC foreign intelligence collection activities conducted under a ministerial directive and ministerial authorizations (Activity 3) /14
- Review of CSEC's acquisition and implementation of technologies as a means to protect the privacy of Canadians /15
- Review of disclosure of information about Canadians to Government of Canada clients /17

- Follow-up to a recommendation in a 2007–2008 review of CSEC activities carried out under a ministerial directive /18
- Review of CSEC activities conducted under a ministerial directive and in support of its foreign intelligence collection mandate /19

Reviews Underway and Planned /20

Complaints about CSEC's Activities /21

Duties under the *Security of Information Act* /22

The Commissioner's Office /22
- My office's new status /22
- Canadian Association of Security and Intelligence Studies 2008 Conference /23
- International Intelligence Review Agencies Conference /23
- British Intelligence and Security Committee of Parliamentarians /24

In Closing /24

Annex A: Mandate of the Communications Security Establishment Commissioner /25

Annex B: Classified Reports, 1996–2009 /27

Annex C: Statement of Expenditures, 2008–2009 /31

Annex D: History of the Office of the Communications Security Establishment Commissioner (OCSEC) /33

Annex E: Role and mandate of the Communications Security Establishment Canada (CSEC) /35

Annex F: OCSEC Review Program — Logic Model /37

INTRODUCTION

This is my third report as Communications Security Establishment Commissioner. It is an appropriate time, in my view, to reflect upon the nature of the work in which my office is engaged and the quality of the relationship that has evolved between the Communications Security Establishment Canada (CSEC) and my office.

Decades of legal experience have taught me that the most important element in any relationship is trust. This is true of all relationships, including the one between my office and CSEC. Trust, in my opinion, is not an entitlement. It is something that must be earned through integrity and professionalism. In the case of CSEC, it is also earned by demonstrating commitment to the protection of national security in a way that ensures compliance with the law and respect for the privacy of Canadians. In the case of my office, trust is earned through a rigorous, comprehensive and fair review process.

Due to the nature of its work, CSEC is required to operate largely in secrecy. The role of my office is, in part, to represent the public interest in accountability in a way that optimizes effective review while not restricting unnecessarily CSEC's legislated role.

My predecessors and I have consistently recognized prevention as an important aspect of the Commissioner's legislated role. As such, most recommendations address shortcomings in CSEC's policies, procedures and practices in order to strengthen the compliance framework and reduce any risk to privacy.

While I have, over the past three years, reported that I have found no instances of lack of compliance with the law, there may be, and have been, instances where disagreements with CSEC arise over a particular issue or where I am not satisfied with CSEC's explanation or information. In such cases, I direct my staff to pursue the issue as thoroughly as required. The manner in which such matters are handled can enhance professional trust between organizations.

As my first term draws to a close, I take satisfaction in noting that mutual trust and commitment to shared democratic values have fostered a productive working relationship. I acknowledge the leadership of CSEC which has demonstrated its commitment to lawfulness and protecting privacy.

THE REVIEW ENVIRONMENT

Proposed amendments to the *National Defence Act*

Ensuring the integrity of CSEC's activities and the review process

In last year's report I once again repeated my concern over ambiguities in Part V.I of the *National Defence Act* (*NDA*) with regard to CSEC's foreign intelligence activities under ministerial authorization. I recommended a number of amendments, including one to clarify the term *activity or class of activities*. I also recommended that a definition of the terms *intercept* and *interception* be inserted into the Act. I have shared with government officials these and other proposals for amendments to the *NDA* that I believe worthwhile to enact.

Ministerial authorizations — Did you know?

A ministerial authorization is a written authorization provided by the Minister of National Defence which sets out conditions CSEC must meet so as not to be in contravention of the *Criminal Code* if, in the process of conducting its foreign intelligence collection or information technology security activities, it incidentally intercepts private communications of Canadians. Ministerial authorizations may be approved or renewed for a period not exceeding one year.

Applying a qualified opinion

At the end of the 2008–2009 reporting period, I continue to apply the *interim* solution put in place by my predecessors: that is, to review CSEC's foreign intelligence collection activities under ministerial authorizations on the basis of the *NDA* as it is interpreted by Justice Canada. However, in some important respects, I disagree with that interpretation — as have both my predecessors.

In April 2006, my immediate predecessor noted in his last report as CSE Commissioner that "my one regret will be if I leave this position without a resolution of the legal interpretation issues that have bedevilled this office since December 2001." In my 2007–2008 report, I noted the Government had indicated that legislative amendments would be brought forward "in due course". This has yet to occur. I want to emphasize, however, that the length of time that has passed without producing amended legislation puts at risk the integrity of the review process.

Observations of the Auditor General

I am pleased to see that the Auditor General has commented on this important matter. In a report released on March 31, 2009, she recognized that the implications of the CSE Commissioner's qualified opinion of CSEC's lawfulness, due to ambiguities in CSEC's legislation, "are serious" (Section 1.14 of the *2009 Status Report of the Auditor General of Canada*).

Review cooperation

One issue that remained unresolved in 2008–2009, stemming from Justice Dennis O'Connor's report concerning a new review mechanism for the Royal Canadian Mounted Police's (RCMP) national security activities, is whether there is a need for integrated review of integrated operations among enforcement and intelligence agencies. Justice O'Connor's recommendations included "statutory gateways" to support integrated review. While cooperation among review bodies must be conducted in a manner that respects security requirements, including the *Security of Information Act*, I find no obstacles, legal or otherwise, to

such cooperation, if required. Moreover, I can, and do, review CSEC activities conducted under part (c) of its mandate — which involve requests for assistance to CSEC from the Canadian Security Intelligence Service (CSIS) and the RCMP — to ensure these activities are in compliance with the law.

The O'Connor inquiry included the examination of information sharing between agencies from different countries. This theme has been discussed by Canadian and international scholars. At the annual conference of the Canadian Association of Security and Intelligence Studies (CASIS), held in October 2008, reference was made to an "accountability gap", concerning an absence of cooperation between review bodies of different countries to review information sharing agreements among their respective intelligence agencies. This is a sensitive area but one that is of great interest to me, particularly as it relates to the potential sharing of personal information about Canadians. Within my own jurisdiction, in the coming year, I will be conducting a review of CSEC's activities in this area.

Parliamentary committee involvement

The Government of Canada has called for increased parliamentary involvement in the review of security and intelligence activities. Traditionally, a role for parliamentarians has been clearly established through the mechanism of Parliamentary committees: in the case of my office, it is the Standing Committee on National Defence, to which my public annual report is referred. Since the creation of the CSE Commissioner's office in 1996, the Commissioner has been invited to appear before this committee to discuss his activities and findings and to answer parliamentarians' questions quite infrequently.

Safeguarding privacy: Regular review of identity disclosures

Following my in-depth review of CSEC's disclosure of information about Canadians to Government of Canada clients, completed in December 2008, it was suggested by CSEC that reviews of this kind could be conducted on a regular basis. Since this CSEC activity lies at the heart of my mandate, I believe it is worthwhile to examine it regularly. As a result, my office has arranged with CSEC to begin reviews at regular intervals throughout the coming reporting year.

I believe the nature of this CSEC suggestion, and the manner in which it was presented to my office, speaks to the professional trust that has evolved in the relationship between our respective organizations. It is a positive sign, and one which I am pleased to highlight in this report.

Information about Canadians — Did you know?

When collecting foreign intelligence, CSEC may incidentally acquire information about Canadians. This information may be retained if it is assessed as essential to the understanding of the foreign intelligence. Information about Canadians may be included in foreign intelligence reporting only if it is suppressed (i.e. replaced by a generic reference such as "a Canadian person"). When receiving a subsequent request for disclosure of the details of the suppressed information, CSEC requires federal departments and agencies to explain their authority to request and use this information under their respective mandates and to provide an operational justification of their need to know this information. Only after these conditions have been met will CSEC release the suppressed information.

Briefings from CSEC

My office is briefed regularly on CSEC operational policies and relevant administrative activities. In 2008–2009, my office was also provided with presentations and training in the areas of information management and information technology (IT) databases, on the safeguarding of IT networks of importance to the Government of Canada, and on the status of CSEC's policy framework. In addition, CSEC provided briefings specific to certain reviews prior to those reviews being undertaken.

More effective review through annual roundtables

For the past two years, my staff and CSEC officials have participated in what has become an annual roundtable meeting aimed at optimizing the review process, while minimizing any adverse impact on CSEC's legislated activities. The roundtable meeting is also an opportunity to reinforce open communication and to enhance mutual understanding and trust in the working relationship between the two organizations. These meetings have proven useful in removing obstacles to effective review and will, I am sure, enable us to make progress in the years ahead.

Strengthening lawful compliance

The objective of my review mandate is to assess whether CSEC's activities comply with the law, including the extent to which CSEC has adequate measures to protect the privacy of Canadians. While I am to report to the Minister and to the Attorney General of Canada any instances of non-compliance with the law, I also make it a point, wherever possible, to identify preventive measures that reinforce CSEC's lawful compliance.

One area in which my predecessors and I consistently called for preventive measures is improved information management practices. As we all previously noted, the absence of an adequate records management system impaired CSEC's ability to account for its activities. In response to these concerns, CSEC has taken positive steps to rectify gaps in record management practices. In fact, a new corporate records management system is expected to be fully operational during the 2009–2010 reporting period. CSEC is to be commended for its efforts in this important area.

A comprehensive review process

In its reviews, my office sometimes goes into great depth, observing CSEC operators and analysts first hand to gain better knowledge of their work. This knowledge is particularly important when my staff examine an area in which I have made a recommendation with which CSEC disagrees.

This year, in one such case, which I describe in the section on Review Highlights, I revisited a recommendation relating to privacy, which was made last year. Following completion of a second, focussed review, I retracted that recommendation because I was satisfied that the risk to privacy was minimal and that CSEC had appropriate safeguards in place. I believe this retraction results from a rigourous but fair review approach which, in this instance, recognized the professional manner in which these particular analysts strive to conduct their work.

Implementing recommendations — Did you know?

Since 1997, my office has submitted 52 reports to the Minister, many of which have contained substantial recommendations. CSEC has accepted and implemented and/or is working to address over 90 percent of these recommendations, which speaks to the effectiveness of the review process.

METHODOLOGY

Identifying risks to lawfulness and privacy

A key ingredient in developing a sound review selection process is the identification of activities, practices or procedures that may pose a risk to CSEC's compliance with the law. For example, these can be potential risks identified by my staff from previous or current reviews of CSEC activities, or from briefing sessions given to my staff by CSEC. CSEC may itself also identify potential risks.

In assessing topics for possible review, I instruct my staff to consider questions such as: to what extent is CSEC exposed to risk of unlawful activity in this area, and what is the likelihood that this could occur?; and if it occurs, what is the potential adverse impact?

In addition, my staff developed more detailed criteria in 2008–2009 to help determine the priority in which the identified areas of potential risk will be reviewed. These criteria, which continue to be refined, include: significant changes to authorities; changes to technology; any area that has never been reviewed in-depth, or has not been reviewed in the past four years; a follow-up to a particular recommendation I made previously; and issues arising in the public domain.

Attributes of a good review

In conducting a review, my staff examine all relevant written and electronic records, files, correspondence and other documentation. My staff conduct interviews with CSEC managers and staff involved in the activities being reviewed and visit CSEC facilities to conduct checks, including CSEC databases. The results of reviews are shared with CSEC and, in most instances, CSEC takes action to strengthen compliance with the law or policy.

One of my primary concerns in the review of CSEC activities is ensuring that each review is based upon appropriate evidence to support all findings, conclusions and recommendations. This means that all evidence gathered must be directly *relevant, replicable* and *valid.*

Review evidence — Did you know?

Evidence is information and data that are collected and used to provide a factual basis for developing findings and recommendations against review criteria.

Relevant: refers to the extent to which the information bears a clear and logical relationship to the review objective(s) and criteria. If information is not relevant, it cannot be evidence. *Replicable:* concerns the likelihood of coming up with the same findings if all steps of the review were reproduced. *Valid:* refers to whether the information actually is what it purports to be in relation to the content, origin and timing. As a general principle, the quantity of evidence is sufficient when there is enough to persuade a reasonable person that the review findings and conclusions are valid and the recommendations are appropriate. In order to decide if the collective weight of the evidence is sufficient, I must consider the quality of the evidence gathered, and the cost of obtaining more evidence relative to its likely benefits.

Developing review findings and recommendations

The comparison of evidence gathered against previously established review criteria results in the development of usable findings and recommendations. Review findings confirm whether criteria have been satisfactorily met, or disclose the level, nature and significance of deviations from them. The process of assessing the evidence gathered against criteria is focussed on questions such as: does a deficiency exist between findings and expectations and as established by the review criteria? what is the cause of the deficiency? what are its likely impacts? and can the deficiency be corrected?

2008–2009 REVIEW HIGHLIGHTS

During the 2008–2009 reporting period, my office completed seven reviews on different aspects of CSEC activities. The reviews were carried out under my authority as articulated in paragraph 273.63(2)(a) and subsection 273.65(8) of the *NDA*.

The primary objective of the reviews, consistent with my mandate, was to assess whether the activities complied with the law, including the extent to which CSEC has adequate measures in place to protect the privacy of Canadians. I am able to report that the activities examined in 2008–2009 complied with the law.

With respect to the first three of the reviews listed below, in which I have reviewed different foreign intelligence collection activities conducted under ministerial authorizations, I reiterate that, pending amendments to clarify the *NDA*, these reviews are based on legal interpretation provided to CSEC by Justice Canada.

Reviews of foreign intelligence activities under ministerial authorizations — Common elements

Paragraph 273.64(1)(a) of the *NDA* authorizes CSEC to collect foreign intelligence in accordance with the Government of Canada's intelligence priorities. In the case of each of the CSEC foreign intelligence collection activities reviewed by my office in 2008–2009, CSEC obtained the ministerial authorization pursuant to subsections 273.65(1) and (2) of the *NDA* because, in carrying out the activities, it was possible that CSEC might intercept communications that either originated or terminated in Canada, and which constituted "private communications", as defined in the *Criminal Code*.

The *NDA* requires that foreign intelligence collection activities not be directed at Canadians or any person in Canada (paragraph 273.64(2)(a)), and that they be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information (paragraph 273.64(2)(b)).

Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 1)

Background

This review examined certain CSEC foreign intelligence collection activities conducted under three successive ministerial authorizations in effect between 2004 and 2007. Two previous reviews of these same activities conducted by my office in 1999 and 2005 respectively were taken into consideration.

Findings

Based on the information reviewed and interviews conducted, I found that CSEC's activities were authorized and carried out in accordance with the law, ministerial requirements, and its operational policies and procedures.

However, the review found that additional information should be recorded and reported to the Minister in order to enhance accountability. This additional information concerns the foreign intelligence CSEC collects under this ministerial authorization and which it shares with its principal partners outside Canada. The sharing of information about Canadians is an area that my office will continue to examine.

The review also found that a memorandum of understanding between CSEC and a federal department respecting these activities should be updated to reflect current practices. In the meantime, CSEC agreed to continue to follow the terms of the existing agreement and to document any new understandings.

In addition, my staff identified certain deficiencies in CSEC policies and procedures related to the activities reviewed.

Recommendations

As a result of these findings, I recommended that CSEC adopt and publish additional written guidance respecting the process its analysts are to follow when making targeting decisions. I also recommended that CSEC amend its policy respecting the deletion of private communications recognized by analysts and found to have no foreign intelligence value. The *NDA* requires that an intercepted private communication shall be used or retained only if it is essential to international affairs, defence or security (paragraph 273.65(2)(d)).

I am pleased to note that CSEC accepted the recommendations, and is making improvements in areas where deficiencies were identified, including making changes to its systems.

Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 2)

Background

This review examined certain other CSEC foreign intelligence collection activities conducted under four ministerial authorizations in effect from 2004 to 2007. The review included an examination of CSEC's reporting of the foreign intelligence to its partners in Canada and abroad.

Findings

Based on the information reviewed and interviews conducted, I found that the activities were authorized and complied with the law and with CSEC operational policies and procedures. Personnel responsible for the collection and management of intelligence activities were interviewed and found to be knowledgeable about the legislative authorities, policies and procedures that govern CSEC's collection.

However, the review also found that CSEC did not meet two of the expectations set out in the ministerial authorizations. In one instance, it was noted that CSEC did not meet a requirement to report in a timely manner to the Minister of National Defence following the expiration of the ministerial authorization. My staff found that the report was not received by the Minister's office until almost one year later.

Secondly, it was noted that in one instance CSEC did not report to the Minister an important increase in the number of private communications it inadvertently intercepted. CSEC subsequently provided my office with an explanation for this omission. Nevertheless, in reviewing this issue, I assessed that the information should have been reported in order to meet the ministerial expectation.

My report to the Minister of National Defence also suggested that CSEC introduce a greater degree of rigour in methodology applied to assessing the value of foreign intelligence reporting.

Recommendation

In addressing the expectation regarding private communications, I recommended that CSEC make an explicit statement to address each ministerial expectation separately in future reports to the Minister. I am pleased to note that CSEC accepted this recommendation.

Review of CSEC foreign intelligence collection activities conducted under a ministerial directive and ministerial authorizations (Activity 3)

Background

This review examined a third type of CSEC foreign intelligence collection activity conducted under three successive ministerial authorizations in effect from 2004 to 2007. In addition, the review examined CSEC's compliance with the expectations set out in a related ministerial directive, issued pursuant to subsection 273.62(3) of the *NDA*.

Findings

Based on the information reviewed and interviews conducted, I found that CSEC's activities were authorized and complied with the law. I did, however, set out specific findings and made recommendations that I believe would strengthen CSEC's practices and compliance with its policies and procedures.

The review also found that CSEC did not meet one expectation set out in the ministerial directive. However, practices at the working level resulted in the fulfilment of the intention of that expectation.

Rigorous business practices at the working level throughout the development, approval and execution of these activities give a high level of assurance that the activities are conducted as approved. The review did not find the same level of clarity, rigour and record keeping in some parts of the program management processes. As a consequence, I made three recommendations.

Recommendations

With respect to CSEC not meeting one expectation of the ministerial directive, and to ensure continuity of practice through time and any staff turnover, I recommended that CSEC include certain measures in its policies or procedures.

Second, while CSEC personnel demonstrated a clear understanding of associated policies and procedures, and there was no suggestion of non-compliance, I recommended that written guidelines be put in place to address certain deficiencies in policies and procedures.

Finally, the record of specific activities is comprehensively documented. In contrast, however, the record of decision related to the management of the program is incomplete. I recommended that both components be subject to the proper application of sound records management processes. As I observed previously, CSEC has been implementing a new records management system and is keeping my office informed of progress, which I am following with interest. I am pleased to note that CSEC has accepted these recommendations and is taking measures to address each of them.

Review of CSEC's acquisition and implementation of technologies as a means to protect the privacy of Canadians

Background

My office reviewed CSEC's acquisition and implementation of technologies as a means to protect the privacy of Canadians, in accordance with subsection 273.64(2) of the *NDA*.

Two types of technologies were studied in this review: a foreign intelligence acquisition system and an analytical tool. The foreign intelligence acquisition system is used to acquire, process and collect information from the global information infrastructure. The analytical tool is used to support CSEC's collection of foreign intelligence and to help ensure the protection of electronic information and information infrastructures of importance to the Government of Canada (IT security). My staff observed demonstrations of the two technologies and queried CSEC operators on various aspects of their use.

Findings

Based on the information reviewed and interviews conducted, I found that CSEC's activities were carried out in accordance with the law. CSEC uses these two technologies to fulfill its legislated mandate and demonstrated that it would modify its technologies, if required, to comply with its statutory obligations to protect the privacy of Canadians. The acquisition, implementation and use of these technologies helps CSEC protect the privacy of Canadians by identifying potential private communications as well as personal information about Canadians.

The review found that special attention should be brought to the development of IT security policy instruments so as to ensure that CSEC's guidance in this regard is up-to-date and formalized at the highest level. There was a difference in practices between CSEC's two business-lines (IT security and foreign intelligence collection) with regard to accounting for personal information identified through analysis. CSEC provided a reasonable explanation for this difference.

Recommendation

I made one recommendation regarding requests for foreign intelligence ministerial authorizations. Since there is a risk of intercepting private communications when using the foreign intelligence acquisition system reviewed, a ministerial authorization was required. I recommended that CSEC re-evaluate how it describes foreign intelligence activities in its requests for ministerial authorizations so as to be more precise about the activities the Minister of National Defence is authorizing. I am pleased to note that CSEC accepted the recommendation.

Review of disclosure of information about Canadians to Government of Canada clients

Background

As part of its mandate to provide foreign intelligence in accordance with Government of Canada intelligence priorities, CSEC disseminates classified reports to federal government departments and agencies that have demonstrated requirements for the information, based on their respective mandates. These reports are authored by CSEC as well as allied agencies and may contain suppressed information about Canadians if it is essential to the understanding of the report (see: *Information about Canadians – Did you know?*).

Findings

Based on the information reviewed and interviews conducted, I found that CSEC's activities complied with the law and with its operational policies and procedures. I made no recommendations.

Follow-up to a recommendation in a 2007–2008 review of CSEC activities carried out under a ministerial directive

Background

Last year, I reported on certain activities undertaken by CSEC under a ministerial directive and in support of its foreign intelligence collection mandate. As indicated in my 2007–2008 Annual Report, I suggested that CSEC re-examine its practice that only those private communications recognized by certain staff be accounted for. I recommended that other staff who observe and handle private communications should also be responsible for accounting for them. CSEC did not accept this recommendation, and, as a result, I directed my staff to conduct a follow-up review of these activities.

This second, focussed review, with direction to probe this matter as deeply as necessary, aimed to acquire greater knowledge about this activity, to examine the risk to privacy, and to determine if CSEC's measures to protect the privacy of Canadians were sufficient in this instance.

The goal of this review was ultimately to determine whether my recommendation of 2007–2008 should be maintained, amended or retracted. Review methodology included first-hand observation of the activities of CSEC front-line personnel conducting this activity.

Findings

The review, based on detailed knowledge and understanding of activities observed by my staff, found that CSEC conducts these activities in accordance with the law and ministerial requirements, and in accordance with operational policies and procedures.

Based on the current practices, as observed in detail on two separate occasions, I assessed that the activities examined in this review involve only a low risk to privacy. CSEC staff conducting the activities have a different and lesser potential of affecting the privacy of Canadians than other staff conducting different activities and who are already required to account for private communications.

In addition, I assessed that CSEC has sufficient measures in place to protect the privacy of Canadians during its conduct of these activities. Personnel were aware of and followed operational policies and procedures that provide direction with respect to the protection of the privacy of Canadians.

I am pleased to note that CSEC recently revised its operational policy on this subject to include additional guidance respecting the protection of the privacy of Canadians. Managers routinely and closely monitor compliance with applicable policies and procedures. The people with whom my staff spoke were forthcoming and demonstrated a professional approach.

Therefore, in view of these findings, I retracted my previous recommendation and informed CSEC that I have no expectation of corrective action in regard to these activities.

Review of CSEC activities conducted under a ministerial directive and in support of its foreign intelligence collection mandate

Background

The specific objective of this review was to acquire knowledge of CSEC's activities conducted under a ministerial directive and in support of its foreign intelligence collection mandate. I examined CSEC's compliance with the expectations set out in the ministerial directive and associated policies and procedures. These expectations are administrative in nature and relate primarily to security and risk management.

Findings

Based on the information reviewed and interviews conducted, I found that CSEC's activities were consistent with the foreign intelligence priorities of the Government of Canada, and were carried out in accordance with the law and with CSEC operational policies and procedures. CSEC had also taken specific measures to protect the privacy of Canadians. I also found that, for the most part, CSEC conducted the activities in accordance with expectations set out in the ministerial directive and with associated policies and procedures.

Recommendations

I recommended, however, that CSEC reconcile certain discrepancies between ministerial expectations and its own practices. I also recommended that CSEC review, update and finalize certain key documents respecting these activities, and that it clarify certain terms used in the documents. I believe this will strengthen CSEC's ability to meet the ministerial expectations and therefore enhance accountability. I am awaiting CSEC's response to these recommendations.

REVIEWS UNDERWAY AND PLANNED

I am pleased to note that of the reviews I indicated were underway in my report last year, all were completed, though the results of the comprehensive study of CSEC's information technology security activities will be submitted to the Minister early in the next reporting year. In addition, the examination of certain common practices of CSEC related to its mandated activities, has been split into several reviews to permit more detailed examination. The first of these, on disclosure of information about Canadians, was completed and submitted to the Minister in this reporting year.

Other reviews that are underway or planned for the next reporting year include: CSEC's foreign intelligence sharing with international partners; activities conducted under foreign intelligence ministerial authorizations; activities conducted under IT security ministerial authorizations; the process by which CSEC determines that targets of foreign intelligence interest are indeed foreign entities located outside Canada, as required by law; and CSEC's assistance (under part (c) of its mandate) to the Canadian Security Intelligence Service under section 16 of the *CSIS Act*.

Some of these reviews may carry over into the 2010–2011 reporting year. There may also be a certain area or activity that, as a result of various factors, I determine to be a priority, resulting in it being reviewed sooner rather than later. This situation is part of the ongoing process of assessing where risks to lawful compliance or privacy are greatest.

COMPLAINTS ABOUT CSEC'S ACTIVITIES

My mandate includes undertaking any investigation I deem necessary in response to a complaint in order to determine whether CSEC engaged, or is engaging, in unlawful activity.

This year my office received one complaint warranting investigation. While I cannot speak to the substance of the complaint, I am able to report that the investigation found no unlawful activity on the part of CSEC.

DUTIES UNDER THE *SECURITY OF INFORMATION ACT*

I have a duty under the *Security of Information Act* to receive information from persons who are permanently bound to secrecy and seek to defend the release of classified information about CSEC on the grounds that it is in the public interest. No such matters were reported to my office in the 2008–2009 reporting period.

THE COMMISSIONER'S OFFICE

During 2008–2009, I met periodically with the Chief of CSEC to discuss issues of mutual interest. These collaborative meetings reflect a productive working relationship which, I believe, contributes to the overall efficiency and effectiveness of the review process.

I had occasion during the reporting period to meet the Prime Minister's newly appointed National Security Advisor, whose duties include accountability for CSEC policy and operational direction. I also met with several federal court judges and other senior government officials.

My office's new status

As I observed in my last report, a decision was taken in the autumn of 2007 that would sever my office's long-standing relationship with the Privy Council Office for the provision of administrative and other support activities and transfer these responsibilities to the Department of National Defence.

Subsequently, it was determined that positioning my office within the same portfolio as CSEC did not have the appearance of propriety and autonomy that ought to exist between an agency and its review body. As a result, and effective April 1, 2009, my office was granted its own parliamentary appropriation. While the reporting relationship to the Minister of National Defence remains intact, as set out in the *NDA*, my office is separate from, and is not part of, that department.

These changes have, by necessity, given rise to additional expenditures for support services, with a corresponding increase in the budget which appears at Annex C. Still, I view this new status as another indication of the maturation of my office and further reinforcement of its independence.

Canadian Association of Security and Intelligence Studies 2008 Conference

My office's participation in the annual CASIS conference in October 2008 afforded an excellent opportunity to exchange perspectives on security and intelligence issues, including review, with leading experts, scholars, policy makers and practitioners from across the country. My office was also pleased to mentor two Canadian graduate students in security and intelligence studies in conference events and discussions.

International Intelligence Review Agencies Conference

I attended the International Intelligence Review Agencies Conference in Auckland, New Zealand in October 2008 to make a presentation to a conference panel on developing trust between a review body and the agency being reviewed, while retaining independence. In my remarks, I emphasized that building and maintaining CSEC's trust in my office, while safeguarding my office's independence, requires constant management and accommodation of interests at all levels.

I also emphasized that CSEC's trust in the Commissioner's office depends significantly on the demonstrable quality of its review work. As a result, my office has placed considerable emphasis on developing, documenting and implementing sound methodologies, based on accepted standards of review and informed by years of practical experience. I added that my office has developed operational policies and procedures that, among other things, provide guidance to staff in carrying out reviews, ensure a large measure of transparency and consistency in my office's work when seen from CSEC's perspective, and provide a basis for assessing and improving CSEC's own performance in implementing its mandate.

British Intelligence and Security Committee of Parliamentarians

I met with the British Intelligence and Security Committee of Parliamentarians during the Committee's visit to Ottawa in March 2009. Committee members and my staff and I participated in a useful exchange of information and opinions on security and intelligence review issues of mutual interest and concern.

IN CLOSING

As I conclude my first term as CSE Commissioner and prepare to embark upon a second term in August 2009 for one year, I do so with satisfaction in current achievements and a sense of optimism going forward. Over the past three years I am pleased to have established a productive working relationship with the Chief of CSEC. I look forward to building on this relationship as I continue to review CSEC's activities in accordance with my mandate. For me, comprehensive review of these activities remains both a challenging and rewarding task, and one which I am greatly honoured to carry out on behalf of Canadians.

ANNEX A: MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

***National Defence Act* – Part V.1**

273.63 (1) The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment to hold office, during good behaviour, for a term of not more than five years.

(2) The duties of the Commissioner are

(a) to review the activities of the Establishment to ensure that they are in compliance with the law;

(b) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and

(c) to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.

(3) The Commissioner shall, within 90 days after the end of each fiscal year, submit an annual report to the Minister on the Commissioner's activities and findings, and the Minister shall cause a copy of the report to be laid before each House of Parliament on any of the first 15 days on which that House is sitting after the Minister receives the report.

(4) In carrying out his or her duties, the Commissioner has all the powers of a commissioner under Part II of the *Inquiries Act*.

(5) The Commissioner may engage the services of such legal counsel, technical advisers and assistants as the Commissioner considers necessary for the proper performance of his or her duties and, with the approval of the Treasury Board, may fix and pay their remuneration and expenses.

(6) The Commissioner shall carry out such duties and functions as are assigned to the Commissioner by this Part or any other Act of Parliament, and may carry out or engage in such other related assignments or activities as may be authorized by the Governor in Council.

(7) The Commissioner of the Communications Security Establishment holding office immediately before the coming into force of this section shall continue in office for the remainder of the term for which he or she was appointed.

[...]

273.65 (8) The Commissioner of the Communications Security Establishment shall review activities carried out under an authorization issued under this section to ensure that they are authorized and report annually to the Minister on the review.

Security of Information Act

15. (1) No person is guilty of an offence under section 13 or 14 if the person establishes that he or she acted in the public interest. [...]

(5) A judge or court may decide whether the public interest in the disclosure outweighs the public interest in non-disclosure only if the person has complied with the following: [...]

(b) the person has, if he or she has not received a response from the deputy head or the Deputy Attorney General of Canada, as the case may be, within a reasonable time, brought his or her concern to, and provided all relevant information in the person's possession to, [...]

(ii) the Communications Security Establishment Commissioner, if the person's concern relates to an alleged offence that has been, is being or is about to be committed by a member of the Communications Security Establishment, in the purported performance of that person's duties and functions of service for, or on behalf of, the Communications Security Establishment, and he or she has not received a response from the Communications Security Establishment Commissioner within a reasonable time.

ANNEX B: CLASSIFIED REPORTS, 1996–2009

1. Principal vs. agent status – March 3, 1997 (TOP SECRET)

2. Operational policies with lawfulness implications – February 6, 1998 (SECRET)

3. CSE's activities under *** – March 5, 1998 (TOP SECRET Codeword/CEO)

4. Internal investigations and complaints – March 10, 1998 (SECRET)

5. CSE's activities under *** – December 10, 1998 (TOP SECRET/CEO)

6. On controlling communications security (COMSEC) material – May 6, 1999 (TOP SECRET)

7. How we test (A classified report on the testing of CSE's signals intelligence collection and holding practices, and an assessment of the organization's efforts to safeguard the privacy of Canadians) – June 14, 1999 (TOP SECRET Codeword/CEO)

8. A study of the *** collection program – November 19, 1999 (TOP SECRET Codeword/CEO)

9. On *** – December 8, 1999 (TOP SECRET/COMINT)

10. A study of CSE's *** reporting process — an overview (Phase I) – December 8, 1999 (SECRET/CEO)

11. A study of selection and *** — an overview – May 10, 2000 (TOP SECRET/CEO)

12. CSE's operational support activities under *** — follow-up – May 10, 2000 (TOP SECRET/CEO)

13. Internal investigations and complaints — follow-up – May 10, 2000 (SECRET)

14. On findings of an external review of CSE's ITS program – June 15, 2000 (SECRET)

15. CSE's policy system review – September 13, 2000 (TOP SECRET/CEO)

16. A study of the *** reporting process — *** (Phase II) – April 6, 2001 (SECRET/CEO)

17. A study of the *** reporting process — *** (Phase III) – April 6, 2001 (SECRET/CEO)

18. CSE's participation *** – August 20, 2001 (TOP SECRET/CEO)

19. CSE's support to ***, as authorized by *** and code-named *** – August 20, 2001 (TOP SECRET/CEO)

20. A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) – August 21, 2002 (SECRET)

21. CSE's support to ***, as authorized by *** and code-named *** – November 13, 2002 (TOP SECRET/CEO)

22. CSE's *** activities carried out under the *** 2002 *** Ministerial authorization – November 27, 2002 (TOP SECRET/CEO)

23. Lexicon of CSE definitions – March 26, 2003 (TOP SECRET)

24. CSE's activities pursuant to *** Ministerial authorizations including *** – May 20, 2003 (SECRET)

25. CSE's support to ***, as authorized by *** and code-named *** — Part I – November 6, 2003 (TOP SECRET/COMINT/CEO)

26. CSE's support to ***, as authorized by *** and code-named *** — Part II – March 15, 2004 (TOP SECRET/COMINT/CEO)

27. A review of CSE's activities conducted under *** Ministerial authorization – March 19, 2004 (SECRET/CEO)

28. Internal investigations and complaints — follow-up – March 25, 2004 (TOP SECRET/CEO)

29. A review of CSE's activities conducted under 2002 *** Ministerial authorization – April 19, 2004 (SECRET/CEO)

30. Review of CSE *** operations under Ministerial authorization – June 1, 2004 (TOP SECRET/COMINT)

31. CSE's support to *** – January 7, 2005 (TOP SECRET/COMINT/CEO)

32. External review of CSE's *** activities conducted under Ministerial authorization – February 28, 2005 (TOP SECRET/COMINT/CEO)

33. A study of the *** collection program – March 15, 2005 (TOP SECRET/COMINT/CEO)

34. Report on the activities of CSE's *** – June 22, 2005 (TOP SECRET)

35. Interim report on CSE's *** operations conducted under Ministerial authorization – March 2, 2006 (TOP SECRET/COMINT)

36. External review of CSE *** activities conducted under Ministerial authorization – March 29, 2006 (TOP SECRET/CEO)

37. Review of CSE's foreign intelligence collection in support of the RCMP (Phase II) – June 16, 2006 (TOP SECRET/COMINT/CEO)

38. Review of information technology security activities at a government department under ministerial authorization – December 18, 2006 (TOP SECRET)

39. Review of CSE signals intelligence collection activities conducted under ministerial authorizations (Phase I) – February 20, 2007 (TOP SECRET/COMINT/CEO)

40. Role of the CSE's client relations officers and the Operational Policy Section in the release of personal information – March 31, 2007 (TOP SECRET/COMINT/CEO)

41. Review of information technology security activities at a government department under ministerial authorization – July 20, 2007 (TOP SECRET)

42. Review of CSEC's counter-terrorism activities – October 16, 2007 (TOP SECRET/ COMINT/CEO)

43. Review of CSE's activities carried out under a ministerial directive – January 9, 2008 (TOP SECRET/COMINT/CEO)

44. Review of CSEC's support to CSIS – January 16, 2008 (TOP SECRET/ COMINT/ CEO)

45. Review of CSEC signals intelligence collection activities conducted under ministerial authorizations (Phase II) – March 28, 2008 (TOP SECRET/ COMINT/CEO)

46. Review of CSEC's acquisition and implementation of technologies as a means to protect the privacy of Canadians – June 11, 2008 (TOP SECRET/COMINT/CEO)

47. Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 1) – June 11, 2008 (TOP SECRET/ COMINT/CEO)

48. Review of disclosure of information about Canadians to Government of Canada clients – November 19, 2008 (TOP SECRET/COMINT/CEO)

49. Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 2) – January 13, 2009 (TOP SECRET/ COMINT/CEO)

50. Review of CSEC foreign intelligence collection activities conducted under a ministerial directive and ministerial authorizations (Activity 3) – February 26, 2009 (TOP SECRET/COMINT/CEO)

51. Review of CSEC activities conducted under a ministerial directive and in support of its foreign intelligence collection mandate – March 12, 2009 (TOP SECRET/ COMINT Codeword/CEO)

52. Follow-up to a recommendation in a 2007–2008 review of CSEC activities carried out under a ministerial directive – March 12, 2009 (TOP SECRET/ COMINT/CEO)

ANNEX C: STATEMENT OF EXPENDITURES 2008-2009

Standard Object Summary

Salaries and Wages	$782,686
Transportation and Telecommunications	43,337
Information	16,303
Professional and Special Services	258,294
Rentals	157,371
Purchased Repair and Maintenance	1,913
Materials and Supplies	7,822
Acquisition of Machinery and Equipment	23,595
Other Expenditures	0
Total	**$1,291,321**

ANNEX D: HISTORY OF THE OFFICE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER (OCSEC)

The Office of the Communications Security Establishment Commissioner (OCSEC) was created on June 19, 1996, with the appointment of the inaugural Commissioner, the Honourable Claude Bisson, O.C., a former Chief Justice of Québec, who held the position until June 2003. He was succeeded by the late Right Honourable Antonio Lamer, P.C., C.C., C.D., LL.D., D.U., former Chief Justice of Canada for a term of three years. The Honourable Charles D. Gonthier, C.C., Q.C., who retired as Justice of the Supreme Court of Canada in 2003, was appointed as Commissioner in August 2006.

For the first six years (from June 1996 to December 2001), the Commissioner carried out his duties under the authority of Orders in Council issued pursuant to Part II of the *Inquiries Act*. During this period, the Commissioner's responsibilities were twofold: to review the activities of the Communications Security Establishment Canada (CSEC) to determine whether they conformed with the laws of Canada; and to receive complaints about CSEC's activities.

Following the terrorist attacks in the United States on September 11, 2001, Parliament adopted the omnibus *Anti-terrorism Act* which came into force on December 24, 2001. The omnibus *Act* introduced amendments to the *National Defence Act*, by adding Part V.1 and creating legislative frameworks for both OCSEC and CSEC. It also gave the Commissioner new responsibilities to review activities carried out by CSEC under a ministerial authorization.

The omnibus legislation also introduced the *Security of Information Act*, which replaced the *Official Secrets Act*. This legislation gives the Commissioner specific duties in the event that a person, who would otherwise be permanently bound to secrecy, seeks to defend the release of classified information about CSEC on the grounds that it is in the public interest. The legislation also continued the Commissioner's powers under the *Inquiries Act*.

In autumn 2007, a decision was taken that would sever OCSEC's long-standing arrangements with the Privy Council Office for administrative and other support activities. Effective April 1, 2009, OCSEC was granted its own parliamentary appropriation. While the Commissioner continues to provide the Minister of National Defence with his reports, OCSEC is separate from, and not part of, the department.

ANNEX E: ROLE AND MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT CANADA (CSEC)

The Communications Security Establishment Canada (CSEC) is Canada's national cryptologic agency. Unique within Canada's security and intelligence community, CSEC employs code-makers and code-breakers to provide the Government of Canada with information technology security and foreign intelligence services. CSEC also provides technical and operational assistance to federal law enforcement and security agencies.

CSEC's foreign intelligence products and services support government decision-making in the fields of national security, national defence and foreign policy. CSEC's signals intelligence activities relate exclusively to foreign intelligence and are directed by the Government of Canada's intelligence priorities.

CSEC's information technology security products and services enable its clients (government departments and agencies) to effectively secure their electronic information systems and networks. CSEC also conducts research and development on behalf of the Government of Canada in fields related to communications security.

CSEC has a three-part mandate under subsection 273.64(1) of the *National Defence Act*. These are known as parts (a), (b) and (c) of its mandate:

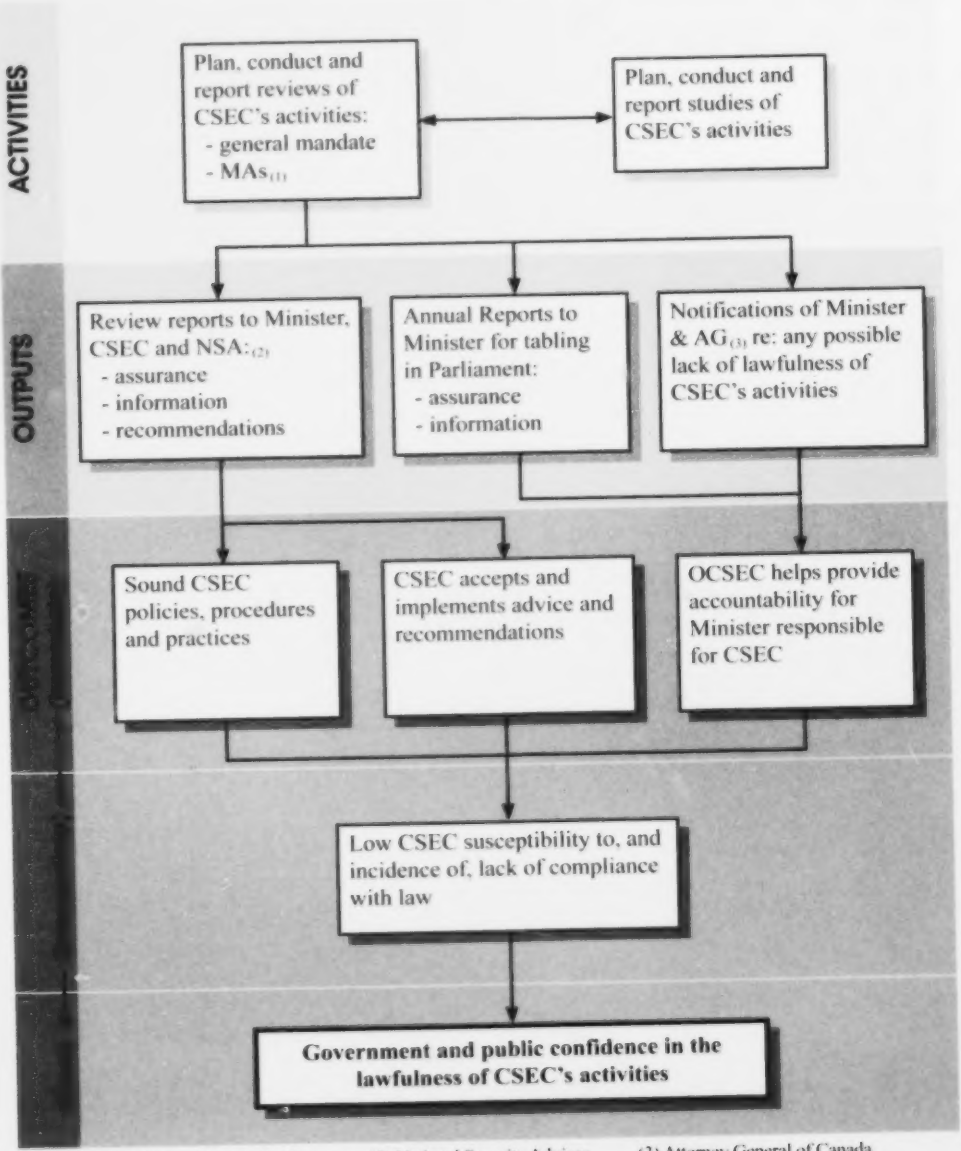
(a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;

(b) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and

(c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

ANNEX F: OCSEC REVIEW PROGRAM — LOGIC MODEL

The following logic model provides a graphic description of how the review program functions.


ACTIVITIES
Plan, conduct and report reviews of CSEC's activities:
- general mandate
- MAs(1)
Plan, conduct and report studies of CSEC's activities
OUTPUTS
Review reports to Minister, CSEC and NSA:(2)
- assurance
- information
- recommendations
Annual Reports to Minister for tabling in Parliament:
- assurance
- information
Notifications of Minister & AG(3) re: any possible lack of lawfulness of CSEC's activities
Sound CSEC policies, procedures and practices
CSEC accepts and implements advice and recommendations
OCSEC helps provide accountability for Minister responsible for CSEC
Low CSEC susceptibility to, and incidence of, lack of compliance with law
Government and public confidence in the lawfulness of CSEC's activities

(1) Ministerial authorizations (2) National Security Advisor to the Prime Minister (3) Attorney General of Canada

Commissaire
du Centre
de la sécurité
des télécommunications

Rapport annuel

2008-2009

Bureau du commissaire du Centre
de la sécurité des télécommunications
C.P. 1984, Succursale « B »
Ottawa (Ontario)
K1P 5R5

Tél. : (613) 992-3044
Téléc. : (613) 992-4096
Site Web : www.ocsec-bccst.gc.ca

© Ministre des Travaux publics et des
Services gouvernementaux Canada 2009
ISBN 978-0-662-06812-9
N° de cat. D95-2009

Photos de la couverture : Malak

FSC
Sources Mixtes

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Charles D. Gonthier, C.C., c.r.

Communications Security
Establishment Commissioner

The Honourable Charles D. Gonthier, C.C., Q.C.

Juin 2009

Ministre de la Défense nationale
Édifice MGen G.R. Pearkes, 13e étage
101, promenade Colonel-By, tour nord
Ottawa (Ontario)
K1A 0K2

Monsieur le ministre,

Conformément au paragraphe 273.63(3) de la *Loi sur la défense nationale*, j'ai le plaisir de vous communiquer mon rapport annuel de 2008–2009 sur mes activités et constatations, aux fins de présentation au Parlement.

Je vous prie d'agréer, monsieur le ministre, l'assurance de ma haute considération.

Charles D. Gonthier

P.O. Box/C.P. 1984, Station "B"/Succursale « B »
Ottawa, Canada
K1P 5R5
(613) 992-3044 Téléc. : (613) 992-4096

TABLE DES MATIÈRES

Introduction /1

Contexte de l'examen /2
- Modifications proposées à la *Loi sur la défense nationale* /2
  - Assurer l'intégrité des activités du CSTC et du processus d'examen /2
  - Une réserve relative à l'examen /3
  - Observations de la vérificatrice générale /3
- Collaboration aux fins de l'examen /3
- Participation du comité parlementaire /4

Rétrospective de l'année /5
- Protection de la vie privée : Examen périodique des divulgations d'identités /5
- Exposés du CSTC /6
- Table ronde annuelle à l'appui de l'efficacité des examens /6
- Renforcement du respect de la loi /6
- Un processus d'examen approfondi /7

Méthodologie /8
- Cibler les risques pour la légalité et la vie privée /8
- Caractéristiques d'un bon examen /8
  - Formulation des conclusions et des recommandations /8

Points saillants de l'examen 2008–2009 /10
- Examens d'activités entreprises en vertu d'autorisations ministérielles — Éléments communs /10
- Examen des activités de collecte de renseignements étrangers menées par le CSTC en vertu d'une autorisation ministérielle (activité 1) /11
- Examen des activités de collecte de renseignements étrangers menées par le CSTC en vertu d'une autorisation ministérielle (activité 2) /12
- Examen des activités de collecte de renseignements étrangers menées par le CSTC en vertu d'une directive ministérielle et d'une autorisation ministérielle (activité 3) /14
- Examen de l'acquisition et de la mise en œuvre des technologies par le CSTC comme moyen de protéger la vie privée des Canadiens /15
- Examen de la divulgation de renseignements sur les Canadiens aux clients du gouvernement du Canada /17

- Suivi d'une recommandation découlant de l'examen effectué en 2007–2008 relativement à des activités du CSTC exercées en vertu d'une directive ministérielle /18
- Examen des activités de collecte de renseignements étrangers menées par le CSTC en vertu d'une directive ministérielle et à l'appui de son mandat en matière de collecte de renseignements étrangers /19

Examens en cours ou projetés /20

Plaintes au sujet des activités du CSTC /21

Fonctions exercées en vertu de la *Loi sur la protection de l'information* /22

Le bureau du commissaire /22
- Nouveau statut de mon bureau /22
- Conférence 2008 de l'Association canadienne pour les études de renseignement et de sécurité /23
- Conférence internationale des organismes de surveillance du renseignement /23
- British Intelligence and Security Committee of Parliamentarians /24

Mot de la fin /24

Annexe A : Mandat du commissaire du Centre de la sécurité des télécommunications /25

Annexe B : Rapports classifiés au ministre, 1996–2009 /27

Annexe C : État des dépenses, 2008–2009 /31

Annexe D : Historique du Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST) /33

Annexe E : Rôle et mandat du Centre de la sécurité des télécommunications Canada (CSTC) /35

Annexe F : Programme d'examen du BCCST — Modèle logique /37

INTRODUCTION

Le présent rapport est le troisième que je publie à titre de commissaire du Centre de la sécurité des télécommunications. Le moment est bien choisi, selon moi, pour présenter la nature du travail qu'effectue mon bureau et la qualité des relations qui se sont établies entre ce dernier et le Centre de la sécurité des télécommunications Canada (CSTC).

Plusieurs dizaines d'années d'expérience dans le domaine juridique m'ont appris que l'élément le plus important d'une relation est la confiance. Cela est vrai pour toutes les relations, y compris celles qu'entretiennent mon bureau et le CSTC. D'après moi, la confiance n'est pas un droit. C'est quelque chose que l'on gagne par son intégrité et son professionnalisme. Le CSTC a gagné cette confiance en faisant la preuve d'un engagement envers la protection de la sécurité nationale et en s'acquittant de ce mandat dans le respect de la loi et de la vie privée des Canadiens. Pour mon bureau, la confiance est le fruit d'un processus d'examen rigoureux, approfondi et juste.

En raison de la nature de son travail, le CSTC doit exercer une grande partie de ses activités dans le secret. Le rôle de mon bureau consiste notamment à représenter l'intérêt public dans le cadre de la reddition de comptes d'une façon qui favorise un examen efficace sans toutefois compromettre sans raison la mission confiée au CSTC par la loi.

Mes prédécesseurs et moi-même avons toujours reconnu que la prévention est un aspect important du rôle conféré au commissaire par la loi. De ce fait, la plupart de mes recommandations visent à corriger des lacunes en ce qui a trait aux politiques, aux procédures et aux pratiques du CSTC, afin de renforcer le cadre de conformité et de réduire les risques pour la vie privée.

Au cours des trois dernières années, j'ai indiqué n'avoir trouvé aucun défaut de conformité à la loi. Cependant, il peut arriver (et cela s'est produit) que je sois en désaccord avec le CSTC relativement à un point particulier ou que les justifications ou les renseignements donnés par l'organisme ne me satisfont pas. Dans ces cas, je demande à mon équipe d'examiner la question aussi attentivement qu'il le faut. La façon dont ces questions sont abordées peut raffermir la confiance professionnelle entre les deux organisations.

Alors que mon premier mandat touche à sa fin, je suis heureux de constater que la confiance mutuelle et l'engagement envers des valeurs démocratiques ont nourri une relation de travail productive. Je salue le leadership dont a fait montre le CSTC dans son engagement à se conformer à loi et à protéger la vie privée des citoyens.

CONTEXTE DE L'EXAMEN

Modifications proposées à la *Loi sur la défense nationale*

Assurer l'intégrité des activités du CSTC et du processus d'examen

Dans le rapport de l'année dernière, j'ai réitéré mes inquiétudes au sujet de certaines ambiguïtés dans la partie V.1 de la *Loi sur la défense nationale* (*LDN*) au sujet des activités de renseignement étranger que mène le CSTC en vertu d'une autorisation ministérielle. J'ai recommandé un certain nombre de modifications, dont une visant à préciser les termes *activité* et *catégorie d'activités*. J'ai également recommandé que soient ajoutés à la *Loi* une définition des termes *intercepter* et *interception*. J'ai donc présenté ces modifications à la *LDN*, de même que certaines autres, aux représentants gouvernementaux, parce que j'estime qu'ils sont importants.

Les autorisations ministérielles — Qu'en est-il?

L'autorisation ministérielle est une autorisation écrite du ministre de la Défense nationale, qui établit les conditions que doit respecter le CSTC pour ne pas contrevenir au *Code criminel* dans l'éventualité où il intercepterait par inadvertance des communications privées de Canadiens dans le cadre de sa collecte de renseignements étrangers ou de ses activités liées à la sécurité des technologies de l'information. Ces autorisations peuvent être approuvées ou renouvelées pour une période maximale d'un an.

Une réserve relative à l'examen

Au terme de l'année de référence 2008–2009, je continue d'appliquer la solution *temporaire* mise en place par mes prédécesseurs, soit de procéder à l'examen des activités de collecte de renseignements étrangers menées par le CSTC en vertu d'autorisations ministérielles conformément à l'interprétation de la *LDN* du ministère de la Justice. Mais, à certains égards importants, tout comme mes deux prédécesseurs, je ne suis pas d'accord avec cette interprétation.

Dans son dernier rapport en tant que commissaire du CST en avril 2006, mon prédécesseur immédiat avait écrit : « Mon seul regret serait peut-être de devoir quitter mon poste avant qu'aient pu se régler les problèmes d'interprétation juridique qui compromettent la bonne marche des activités de ce bureau depuis décembre 2001 ». Dans mon rapport de 2007–2008, j'ai noté que le gouvernement avait indiqué que les modifications législatives seraient adoptées « en temps opportun ». Ceci n'a pas encore été fait. Mais je tiens à souligner que le temps qui s'écoule sans qu'on applique les modifications législatives met en danger l'intégrité du processus d'examen.

Observations de la vérificatrice générale

Je suis heureux de constater que la vérificatrice générale a commenté cette question importante. Dans son rapport publié le 31 mars 2009, elle reconnaît que la réserve exprimée par le commissaire du CST au sujet de la légalité des activités du CSTC, en raison des ambiguïtés dans la loi le régissant, « a de sérieuses retombées » (*Rapport* Le Point *de 2009 de la vérificatrice générale du Canada*, mars, section 1.74).

Collaboration aux fins de l'examen

La question de savoir s'il est nécessaire de conclure un protocole d'entente pour l'examen des opérations intégrées entre les organismes d'application de la loi et de collecte du renseignement — qui découlait du rapport du juge Dennis O'Connor sur un nouveau mécanisme d'examen des activités de la Gendarmerie royale du Canada (GRC) en matière de sécurité nationale — n'a pas été réglée en 2008–2009. Le juge O'Connor recommandait entre autres l'instauration de « passerelles législatives » à l'appui d'un examen intégré. Je ne vois aucun obstacle, juridique ou autre,

à une telle collaboration des organismes d'examen, pourvu que celle-ci soit mise en œuvre de manière à respecter les exigences de sécurité, notamment la *Loi sur la protection de l'information*. Par ailleurs, je peux procéder, et je procède à l'examen des activités du CSTC dans le cadre de la troisième partie de son mandat, qui consistent à répondre aux demandes d'assistance du Service canadien du renseignement de sécurité (SCRS) et de la GRC, afin de vérifier si elles sont menées en conformité à la loi.

La commission d'enquête O'Connor comportait également un examen de la mise en commun de renseignements entre les organismes de différents pays. Cette question a déjà été discutée par des spécialistes du Canada et d'ailleurs. Lors de la conférence annuelle de l'Association canadienne pour les études de renseignement et de sécurité, en octobre 2008, il a été question d'un « manque d'imputabilité », du fait de l'absence de coopération entre les organismes d'examen de différents pays dans le cadre de l'examen des ententes d'échange de renseignements entre leur organisme de renseignement respectif. Bien qu'il s'agisse d'une question délicate, elle m'intéresse particulièrement, surtout parce qu'elle concerne l'éventuelle transmission de renseignements personnels sur les Canadiens. Je procéderai, dans le cadre de mes propres pouvoirs, à un examen des activités du CSTC dans ce secteur au cours de la prochaine année.

Participation du comité parlementaire

Le gouvernement du Canada a demandé à ce que le Parlement participe davantage à l'examen des activités de sécurité et de renseignement. Depuis longtemps, le rôle des parlementaires est clairement établi aux termes du mécanisme des comités parlementaires. Or, dans le cas de mon bureau, il s'agit du Comité permanent de la Défense nationale, auquel est soumis mon rapport annuel public. Depuis la création du Bureau du commissaire du CST en 1996, le commissaire n'a pas été invité souvent à témoigner devant ce comité pour discuter de ses activités et de ses constatations, et répondre aux questions des parlementaires.

Protection de la vie privée : Examen périodique des divulgations d'identités

En décembre 2008, mon bureau a achevé un examen approfondi des activités du CSTC concernant la divulgation de renseignements sur les Canadiens aux clients du gouvernement du Canada. À la suite de cet examen, le CSTC a suggéré que mon bureau procède à un examen de ce genre de façon régulière. Puisque cette activité du CSTC est au cœur de mon mandat, je crois qu'il vaut la peine de la soumettre à un examen périodique. Mon bureau a donc pris les dispositions nécessaires avec le CSTC afin que l'on procède à des examens à intervalles réguliers au cours de l'année de référence à venir.

Je suis d'avis que la nature de cette suggestion du CSTC, tout comme la manière dont elle a été présentée à mon bureau, témoigne de la confiance professionnelle qui s'est développée dans la relation entre nos organismes respectifs. Il s'agit là d'un signe positif que je souligne avec plaisir dans ce rapport.

Renseignements sur les Canadiens — Qu'en est-il?

Lorsqu'il collecte des renseignements étrangers, le CSTC peut, par inadvertance, obtenir des renseignements au sujet de Canadiens. Il peut conserver ces renseignements s'il estime qu'ils sont essentiels à la compréhension des renseignements étrangers. Pour inscrire ces renseignements dans des rapports de renseignements étrangers, il doit les supprimer (p. ex., en les remplaçant par un terme générique, comme « un Canadien ou une Canadienne »). Par la suite, s'il reçoit une demande de divulgation des renseignements supprimés, le CSTC exige du ministère ou de l'organisme fédéral qu'il rende compte de son pouvoir de demander et d'utiliser ces renseignements dans le cadre de son mandat et qu'il fournisse une justification opérationnelle de son besoin de connaître ces renseignements. Le demandeur doit satisfaire à toutes ces conditions avant que le CSTC divulgue les renseignements supprimés.

Exposés du CSTC

Le CSTC fournit régulièrement à mon bureau des exposés sur ses politiques opérationnelles et ses activités administratives pertinentes. En 2008–2009, mon bureau a également eu droit à des présentations et à des formations dans les domaines des bases de données relatives à la gestion de l'information et aux technologies de l'information (TI), sur la protection des réseaux TI importants pour le gouvernement du Canada et sur l'état des politiques du CSTC. Le CSTC a en outre donné des exposés particuliers à certains examens, avant le début de ces examens.

Table ronde annuelle à l'appui de l'efficacité des examens

Au cours des deux dernières années, mon équipe et des représentants du CSTC ont participé à ce qui est devenu une table ronde annuelle destinée à optimiser le processus d'examen tout en réduisant les conséquences négatives sur les activités du CSTC prévues par la loi. Cette réunion est aussi l'occasion de renforcer une communication transparente et d'améliorer la compréhension et la confiance mutuelles dans la relation de travail entre les deux organisations. Ces réunions ont permis d'éliminer des obstacles à l'efficacité des examens et nous permettront, j'en suis convaincu, de réaliser des progrès au cours des années à venir.

Renforcement du respect de la loi

Mon mandat d'examen a pour objectif d'évaluer si les activités du CSTC respectent la loi et si l'organisme est doté de mesures suffisantes pour protéger la vie privée des Canadiens. Je suis naturellement tenu d'informer le ministre et le procureur général du Canada de toute situation de non-conformité à la loi. Cependant, je me fais aussi un devoir de proposer, aussi souvent que possible, des mesures préventives visant à renforcer le respect de la loi par le CSTC.

La question de l'amélioration des pratiques de gestion de l'information en est une pour laquelle mes prédécesseurs et moi-même avons invariablement demandé que des mesures préventives soient prises. Comme nous l'avons tous indiqué, l'absence d'un système approprié de gestion des documents a entravé le CSTC dans sa capacité de rendre compte de ses activités.

Il a pris des mesures positives afin de combler ses lacunes en la matière. En fait, un nouveau système ministériel de gestion des dossiers devrait être mis en place au cours de l'année de référence 2009–2010. Le CSTC mérite des éloges pour ses efforts dans ce secteur important.

Un processus d'examen approfondi

Lorsqu'ils procèdent à un examen, les membres de mon équipe approfondissent parfois beaucoup leurs recherches et vont observer directement les opérateurs et les analystes du CSTC, afin de mieux comprendre leur travail. Ces connaissances sont particulièrement importantes lorsqu'ils examinent un élément au sujet duquel j'ai fait une recommandation avec laquelle le CSTC est en désaccord.

Une telle situation s'est présentée cette année — il en est question à la section Points saillants de l'examen — et j'ai révisé une recommandation sur la vie privée que j'avais formulée l'année dernière. Ainsi, à la suite d'un deuxième examen approfondi, j'ai rétracté ma recommandation parce que j'ai été convaincu que le risque pour la vie privée était minime et que le CSTC disposait de mesures de protection adéquates. Je pense que cette rétractation découle d'une approche rigoureuse, mais juste, en matière d'examen qui, dans ce cas, reconnaît le professionnalisme que s'efforcent d'appliquer les analystes concernés.

Mise en œuvre des recommandations — Qu'en est-il?

Depuis 1997, mon bureau a présenté 52 rapports au ministre. La plupart de ceux-ci comportaient nombre de recommandations. Le CSTC a accepté et mis en œuvre (ou il travaille à appliquer) plus de 90 p. 100 de ces recommandations, ce qui témoigne de l'efficacité du processus d'examen.

MÉTHODOLOGIE

Cibler les risques pour la légalité et la vie privée

Pour élaborer un processus solide de sélection des examens, il est important de cerner les activités, les pratiques et les procédures qui risquent de compromettre le respect de la loi par le CSTC. Par exemple, il arrive que mon équipe repère des risques éventuels à partir d'examens des activités du CSTC qui sont terminés ou en cours ou lors des séances d'information que donne l'organisme. En outre, le CSTC peut lui-même détecter des risques éventuels.

Lorsque j'évalue des sujets pouvant faire l'objet d'un examen, je demande à mon équipe de se pencher sur des questions comme : à quel point le CSTC est-il exposé au risque d'activités illégales dans ce secteur et quelle est la probabilité que cela survienne? Et si cela survient, quelle en est l'incidence négative probable?

Par ailleurs, en 2008–2009, mon équipe a défini des critères détaillés permettant d'établir l'ordre de priorité dans lequel il examinera les risques éventuels. Ces critères, qui font continuellement l'objet d'améliorations, sont notamment les suivants : des modifications importantes des pouvoirs conférés par la loi; des modifications de la technologie; le fait qu'un secteur n'ait jamais fait l'objet d'un examen approfondi ou qu'il n'ait pas été examiné au cours des quatre dernières années; le suivi d'une recommandation faite auparavant; et des problèmes qui surviennent dans le domaine public.

Caractéristiques d'un bon examen

Dans le cadre d'un examen, mon personnel examine tous les dossiers, fichiers, correspondance et autres documents écrits et électroniques se rapportant à l'activité en question. Il s'entretient avec les gestionnaires et les employés du CSTC qui ont participé aux activités visées par l'examen et se rend dans les locaux de l'organisme afin de procéder à des vérifications, y compris celles de ses bases de données. Les résultats de l'examen sont présentés au CSTC qui, dans la plupart des cas, prend des mesures afin de renforcer son respect de la loi ou des politiques.

À mon avis, un aspect très important de chaque examen des activités du CSTC est de faire en sorte que toutes les constatations, conclusions et recommandations de mon bureau soient étayées par des preuves solides. Autrement dit, chaque élément recueilli doit être directement *pertinent*, *reproductible* et *valable*.

Preuve d'examen — Qu'en est-il?

La preuve est constituée des renseignements et des données que l'on collecte et utilise à titre de fondements factuels pour formuler des conclusions et des recommandations au regard des critères de l'examen.

Pertinent : il existe une relation claire et logique entre les renseignements obtenus et les objectifs et critères de l'examen. Si les renseignements ne sont pas pertinents, ils ne peuvent être utilisés comme preuve; *reproductible* : il est probable qu'on obtiendrait les mêmes résultats si toutes les étapes de l'examen étaient répétées; *valable* : l'information est bien ce qu'elle est censée être relativement à son contenu, à son origine et au moment où elle a été recueillie. En général, la preuve recueillie est suffisante lorsqu'on a assez d'éléments pour convaincre une personne raisonnable de la validité des observations et des conclusions de l'examen et de la pertinence des recommandations. Pour décider si le poids de la preuve est globalement suffisant, je dois tenir compte de la qualité de la preuve recueillie et du coût lié à l'obtention d'éléments supplémentaires par rapport aux avantages qu'ils apporteraient.

Formulation des conclusions et des recommandations

La comparaison de la preuve recueillie aux critères de l'examen préalablement établis débouche sur la formulation de conclusions et de recommandations utilisables. Les conclusions permettent de confirmer si l'examen a satisfait aux critères, ou, si ce n'est pas le cas, de révéler le niveau, la nature et l'importance des écarts observés. Le processus d'évaluation de la preuve recueillie au regard des critères est fondé sur des questions telles que : les conclusions sont-elles à la hauteur des attentes et des critères de l'examen? S'il y a une lacune, quelle en est la cause? Quelles en sont les conséquences probables? Peut-on corriger la situation?

POINTS SAILLANTS DE L'EXAMEN 2008–2009

Au cours de l'année de référence 2008–2009, mon bureau a effectué sept examens portant sur différents aspects des activités du CSTC, et ce, sous mon autorité comme le prévoient l'alinéa 273.63(2)*a*) et le paragraphe 273.65(8) de la *Loi sur la défense nationale*.

Les examens avaient pour objectif principal d'évaluer, conformément à mon mandat, si les activités du CSTC respectaient la loi et en particulier si l'organisme est doté de mesures suffisantes pour protéger la vie privée des Canadiens. Je suis en mesure d'affirmer que les activités ayant fait l'objet d'un examen en 2008–2009 respectaient la loi.

En ce qui concerne les trois premiers examens présentés ci-après (activités 1, 2 et 3), pour lesquels je me suis penché sur diverses activités de collecte de renseignements étrangers menées en vertu d'autorisations ministérielles, je tiens à souligner de nouveau que ces examens sont fondés sur l'interprétation juridique que le ministère de la Justice a fournie au CSTC, en attendant que la *Loi sur la défense nationale* soit modifiée.

Examens d'activités entreprises en vertu d'autorisations ministérielles — Éléments communs

En vertu de l'alinéa 273.64(1)*a*) de la *Loi*, le CSTC a pour mandat d'acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignement. Pour chaque activité de collecte de renseignements étrangers menée par le CSTC examinée par mon bureau en 2008–2009, le CSTC a obtenu une autorisation ministérielle en vertu des paragraphes 273.65(1) et (2) de la *Loi* étant donné qu'il était possible qu'il intercepte, dans le cadre de ces travaux, des communications provenant du Canada ou destinées au Canada considérées comme des « communications privées » aux termes du *Code criminel*.

Selon la *Loi sur la défense nationale*, les activités de collecte de renseignements étrangers ne peuvent viser des Canadiens ou toute personne au Canada (alinéa 273.64(2)*a*) et doivent être soumises à des mesures de protection de la vie privée des Canadiens lors de l'utilisation et de la conservation des renseignements interceptés (alinéa 273.64(2)*b*).

Examen des activités de collecte de renseignements étrangers menées par le CSTC en vertu d'une autorisation ministérielle (activité 1)

Contexte

Cet examen touchait certaines activités de collecte de renseignements étrangers menées par le CSTC en vertu de trois autorisations ministérielles successives en vigueur entre 2004 et 2007. On a pris en compte deux examens des mêmes activités, réalisés par mon bureau en 1995 et en 2005.

Conclusions

À la lumière des renseignements examinés et des entrevues, j'ai conclu que les activités du CSTC avaient été autorisées et menées conformément à la loi, aux exigences ministérielles ainsi qu'aux politiques et procédures opérationnelles de l'organisme.

Cependant, il en est ressorti que l'imputabilité du CSTC au ministre serait meilleure s'il consignait et rapportait davantage d'information. Cette information concerne les renseignements étrangers que le CSTC collecte en vertu de son autorisation ministérielle et qu'il communique à ses principaux partenaires à l'extérieur du Canada. Mon bureau continuera d'examiner la question d'échange de renseignements sur les Canadiens.

L'examen a également révélé qu'un protocole d'entente entre le CSTC et un ministère fédéral concernant ces activités devrait être mis à jour de sorte qu'il soit conforme aux pratiques actuelles. Dans l'intervalle, le CSTC a convenu de continuer à respecter les modalités de l'entente actuelle et à consigner toute nouvelle entente.

En outre, les membres de mon équipe ont signalé certaines irrégularités liées aux politiques et aux procédures du CSTC relatives aux activités examinées.

Recommandations

Par suite de ces constatations, j'ai recommandé au CSTC d'adopter et de publier des directives écrites supplémentaires touchant les procédures que doivent suivre ses analystes lorsqu'ils prennent des décisions relativement aux cibles. J'ai également conseillé au CSTC de modifier sa politique en matière de radiation des communications privées qui, selon les analystes, n'ont aucune valeur sur le plan des renseignements étrangers. La *LDN* stipule que les communications privées interceptées ne seront utilisées ou conservées que si elles sont essentielles aux affaires internationales, à la défense ou à la sécurité (alinéa 273.65(2)*d*).

Je suis heureux de constater que le CSTC a accepté mes recommandations et apporté des améliorations dans les domaines où nous avons relevé des carences, notamment la modification de ses systèmes.

Examen des activités de collecte de renseignements étrangers menées par le CSTC en vertu d'une autorisation ministérielle (activité 2)

Contexte

Cet examen touchait certaines autres activités de collecte de renseignements étrangers menées par le CSTC en vertu de quatre autorisations ministérielles en vigueur de 2004 à 2007, y compris l'échange par le CSTC de renseignements étrangers à ses partenaires au Canada et à l'étranger.

Conclusions

Selon les renseignements examinés et les entrevues, j'ai conclu que les activités étaient autorisées et conformes à la loi ainsi qu'aux politiques et aux procédures opérationnelles du CSTC. Les entrevues ont permis

d'établir que les employés chargés de la collecte des renseignements et de la gestion des activités connexes connaissaient bien les autorisations législatives, les politiques et les procédures qui régissent la collecte de renseignements par le CSTC.

Toutefois, l'examen a également permis d'établir que le CSTC n'avait pas respecté deux des attentes énoncées dans les autorisations ministérielles. Dans un cas, j'ai noté que le CSTC n'avait pas respecté une exigence relative à la présentation d'un rapport en temps opportun au ministre de la Défense nationale, après l'expiration de l'autorisation ministérielle. Mon équipe a constaté que le bureau du ministre avait reçu ledit rapport près d'un an plus tard.

J'ai en outre constaté que, dans un cas, le CSTC n'avait pas informé le ministre d'une augmentation marquée du nombre de communications privées interceptées par inadvertance. Par la suite, l'organisme nous a fourni une explication à cet égard. Néanmoins, en examinant cette question, j'ai établi que ces renseignements auraient dû être transmis au ministre afin de répondre à ses attentes.

Dans mon rapport au ministre de la Défense nationale, j'ai également recommandé que le CSTC adopte des méthodes plus rigoureuses pour évaluer l'importance des renseignements étrangers fournis à leurs clients.

Recommandations

En ce qui concerne les attentes relatives aux communications privées, j'ai recommandé au CSTC d'élaborer un énoncé explicite relatif à chaque attente ministérielle dans les rapports qu'il présentera au ministre. Je suis heureux de constater que le CSTC a accepté cette recommandation.

Examen des activités de collecte de renseignements étrangers menées par le CSTC en vertu d'une directive ministérielle et d'une autorisation ministérielle (activité 3)

Contexte

Cet examen touchait un troisième type d'activités de collecte de renseignements étrangers menées par le CSTC en vertu de trois autorisations ministérielles successives en vigueur de 2004 à 2007. En outre, l'examen portait sur la conformité du CSTC aux attentes figurant dans une directive ministérielle connexe, émise conformément au paragraphe 273.62(3) de la *LDN*.

Conclusions

En me fondant sur les renseignements examinés et sur les entrevues, j'ai conclu que les activités du CSTC étaient autorisées et conformes à la loi. Toutefois, j'ai présenté des conclusions précises et formulé des recommandations qui, selon moi, permettraient de renforcer les pratiques du CSTC et la conformité à ses politiques et procédures.

L'examen a également permis d'établir que l'organisme n'avait pas respecté une attente énoncée dans la directive ministérielle. Toutefois, les pratiques opérationnelles ont permis de satisfaire aux buts de cette attente.

Des pratiques opérationnelles rigoureuses en matière d'élaboration, d'approbation et d'exécution de ces activités permettent de conclure avec un degré de confiance élevé que ces dernières sont menées conformément aux autorisations. Nous n'avons cependant pas trouvé le même niveau de clarté, de rigueur et de tenue de dossier en ce qui a trait à certaines parties des processus de gestion du programme. Par conséquent, j'ai émis trois recommandations.

Recommandations

En ce qui concerne le non-respect d'une attente figurant dans la directive ministérielle et pour assurer que l'organisme maintienne ses pratiques au fil du temps et malgré le roulement de personnel, j'ai recommandé au CSTC d'ajouter certaines mesures à ses politiques ou procédures.

Deuxièmement, bien que le personnel du CSTC ait montré une bonne compréhension des politiques et procédures connexes et que rien n'indique la non-conformité, j'ai recommandé qu'on établisse des lignes directrices écrites pour combler certaines lacunes des politiques et procédures.

Enfin, le compte rendu d'activités précises est consigné en détail. Par contre, le compte rendu des décisions relatives à la gestion du programme est incomplet. J'ai recommandé qu'on applique correctement à ces deux éléments des processus valables de gestion des documents. Comme je l'ai mentionné précédemment, le CSTC est en train de mettre en œuvre un nouveau système de gestion des documents et il me tient au courant du déroulement de ce projet, que je suis avec intérêt. Je suis heureux de constater que le CSTC a accepté ces recommandations et prend des mesures pour répondre à chacune d'entre elles.

Examen de l'acquisition et de la mise en œuvre des technologies par le CSTC comme moyen de protéger la vie privée des Canadiens

Contexte

Mon bureau a examiné l'acquisition et la mise en œuvre par le CSTC de technologies permettant de protéger la vie privée des Canadiens conformément aux dispositions du paragraphe 273.64(2) de la *LDN*.

L'examen visait deux types de technologies : un système d'acquisition de renseignements étrangers et un outil analytique. Le premier est utilisé pour acquérir, traiter et recueillir des renseignements provenant de l'infrastructure mondiale d'information. Le second appuie la collecte de renseignements étrangers et aide l'organisme à assurer la protection des renseignements électroniques et des infrastructures d'information importantes pour la sécurité du gouvernement du Canada sur le plan des technologies de l'information (sécurité des TI). Les membres de mon équipe ont assisté à des démonstrations touchant les deux technologies et ils ont interrogé les opérateurs du CSTC au sujet de différentes facettes de leur utilisation.

Conclusions

D'après les renseignements examinés et les entrevues, j'ai conclu que les activités du CSTC étaient conformes à la loi. Le CSTC utilise ces deux technologies pour s'acquitter du mandat que lui confère la loi, et il a démontré qu'il modifierait ses technologies le cas échéant pour se conformer à ses obligations statutaires en matière de protection de la vie privée des Canadiens. L'acquisition, la mise en œuvre et l'utilisation de ces technologies aident l'organisme en lui permettant de détecter les communications pouvant être privées ainsi que les renseignements personnels au sujet des Canadiens.

L'examen a révélé que l'élaboration des instruments de politique relatifs à la sécurité des TI devrait faire l'objet d'une attention particulière, pour faire en sorte que les directives du CSTC dans ce domaine soient à jour et officialisés au plus haut niveau. Il existe une différence entre les pratiques relatives aux deux secteurs d'activité du CSTC – la sécurité des TI et la collecte de renseignements étrangers – en ce qui a trait à la reddition de comptes en matière de renseignements personnels détectés au moyen d'analyses. Le CSTC a fourni une explication raisonnable au sujet de cette différence.

Recommandation

J'ai formulé une recommandation au sujet des demandes d'autorisation ministérielle en matière de renseignements étrangers. Comme des communications privées peuvent être interceptées par le système d'acquisition de renseignements étrangers soumis à l'examen, une autorisation ministérielle est nécessaire. J'ai recommandé au CSTC d'examiner de nouveau la façon dont il décrit les activités en matière de renseignements étrangers dans ses demandes d'autorisation ministérielle, afin de mieux préciser les activités que le ministre de la Défense nationale autorise. Je suis heureux de constater que le CSTC a accepté cette recommandation.

Examen de la divulgation de renseignements sur les Canadiens aux clients du gouvernement du Canada

Contexte

Dans le cadre de son mandat visant à fournir des renseignements étrangers conformément aux priorités du gouvernement du Canada en matière de renseignements, le CSTC transmet ses propres rapports classifiés, ainsi que ceux des agences alliées, aux ministères et organismes fédéraux qui ont un besoin prouvé en matière de renseignement, en fonction de leur mandat respectif. Ces rapports sont préparés par le CSTC ainsi que par des partenaires internationaux et ils peuvent contenir des renseignements supprimés au sujet de Canadiens si cela est indispensable à la compréhension du rapport (voir l'encadré *Renseignements sur les Canadiens — Qu'en est-il?*).

Conclusions

À la lumière des renseignements examinés et des entrevues effectuées, j'ai conclu que les activités du CSTC étaient autorisées et conformes à la loi ainsi qu'aux politiques et aux procédures opérationnelles de l'organisme. Je n'ai formulé aucune recommandation.

Suivi d'une recommandation découlant de l'examen effectué en 2007–2008 relativement à des activités du CSTC exercées en vertu d'une directive ministérielle

Contexte

L'an dernier, j'ai présenté mes observations sur certaines activités du CSTC exercées en vertu d'une directive ministérielle et visant à appuyer son mandat en matière de collecte de renseignements étrangers. Comme je l'indiquais dans mon rapport annuel 2007–2008, j'ai recommandé au CSTC de réexaminer sa pratique selon laquelle seulement les communications privées reconnues par certains membres du personnel doivent faire l'objet d'un rapport. J'ai recommandé que d'autres employés qui observent et traitent des communications privées soient également tenus de rendre compte de ces communications. Le CSTC a rejeté cette recommandation, et j'ai donc demandé aux membres de mon équipe de mener un examen de suivi concernant ces activités.

Ce deuxième examen approfondi, assorti d'une directive permettant d'examiner la question de manière aussi approfondie que nécessaire, visait à mieux connaître cette activité, à examiner les risques pour la vie privée et à établir si les mesures prises par le CSTC pour protéger la vie privée des Canadiens étaient suffisantes.

L'examen avait pour objectif ultime de déterminer si je devais maintenir, modifier ou rétracter la recommandation que j'avais formulée en 2007–2008. La méthode d'examen comprenait l'observation directe des activités du personnel de première ligne du CSTC.

Conclusions

L'examen, reposant sur une connaissance et une compréhension précises des activités observées par les membres de mon équipe, a révélé que le CSTC mène ces activités dans le respect de la loi et des exigences ministérielles, et conformément aux politiques et aux procédures opérationnelles.

D'après les pratiques en vigueur, telles qu'elles ont été observées en détail à deux reprises, j'estime que les activités soumises à l'examen ne présentent qu'un faible risque pour la vie privée. Les employés du CSTC qui en sont chargés ont moins de chances de porter atteinte à la vie privée des Canadiens que ceux qui effectuent d'autres activités et qui sont déjà tenus de rendre compte des communications privées.

En outre, j'estime que le CSTC a mis en place des mesures suffisantes afin de protéger la vie privée des Canadiens lorsqu'il mène ces activités. Les employés connaissaient et respectaient les politiques et les procédures opérationnelles dans lesquelles figurent les directives à cet égard.

Je suis heureux de constater que le CSTC a récemment révisé sa politique opérationnelle à ce sujet pour y ajouter des directives supplémentaires en matière de protection de la vie privée des Canadiens. Les gestionnaires surveillent régulièrement et de près la conformité aux politiques et aux procédures applicables. Les personnes à qui les membres de mon équipe ont parlé se sont montrées très ouvertes et ont fait preuve de professionnalisme à l'égard des activités soumises à l'examen.

Ainsi, compte tenu de ces conclusions, j'ai rétracté ma recommandation antérieure et informé le CSTC que je ne m'attends pas à ce qu'il prenne des mesures correctives quant à ces activités.

Examen des activités de collecte de renseignements étrangers menées par le CSTC en vertu d'une directive ministérielle et à l'appui de son mandat en matière de collecte de renseignements étrangers

Contexte

L'objectif précis de cet examen visait à connaître les activités du CSTC menées en vertu d'une autorisation ministérielle et à l'appui de son mandat en matière de collecte de renseignements étrangers. J'ai examiné la conformité du CSTC aux attentes figurant dans la directive ministérielle et aux politiques et procédures connexes. Ces attentes sont de nature administrative et touchent principalement la sécurité et la gestion du risque.

Conclusions

Selon les renseignements examinés et les entrevues menées, j'ai conclu que les activités étaient conformes aux priorités du gouvernement du Canada en matière de renseignements étrangers ainsi qu'à la loi et aux politiques et procédures opérationnelles de l'organisme. Le CSTC avait également pris des mesures précises pour protéger la vie privée des Canadiens. J'ai en outre conclu qu'en général le CSTC menait ses activités conformément aux attentes figurant dans la directive ministérielle et aux politiques et procédures connexes.

Recommandations

Toutefois, j'ai recommandé au CSTC de combler certains écarts entre les attentes ministérielles et ses propres pratiques. J'ai aussi conseillé à l'organisme d'examiner, de mettre à jour et de compléter certains documents clés relatifs à ces activités et de clarifier certains termes y figurant. Je crois que cette mesure permettra au CSTC de mieux répondre aux exigences ministérielles, augmentant ainsi l'imputabilité. J'attends la réponse du CSTC à mes recommandations.

EXAMENS EN COURS OU PROJETÉS

Je suis heureux de constater que les examens en cours figurant dans mon rapport de l'an dernier sont tous terminés; les résultats de l'étude exhaustive des activités du CSTC en matière de sécurité des technologies de l'information sera cependant présentée au ministre au début de la prochaine année de référence. En outre, l'examen de certaines pratiques communes du CSTC touchant les activités prescrites en vertu de son mandat a été scindé en plusieurs examens afin de permettre une étude plus approfondie. Le premier examen, qui portait sur la divulgation de renseignements au sujet de Canadiens, est terminé et a été présenté au ministre pendant la présente année de référence.

Voici les autres examens en cours ou projetés pour la prochaine année : l'échange des renseignements étrangers du CSTC à ses partenaires internationaux; activités menées en vertu d'autorisations ministérielles en matière de renseignements étrangers; activités menées en vertu d'autorisations ministérielles relatives à la sécurité des TI; processus permettant au CSTC d'établir que les cibles de renseignements étrangers sont bien des entités étrangères situées en dehors du Canada, comme le prescrit la *Loi*; assistance du CSTC au Service canadien du renseignement de sécurité (conformément à la partie c) de son mandat) en vertu de l'article 16 de la *Loi sur le service canadien du renseignement de sécurité*.

Certains de ces examens pourraient se poursuivre en 2010–2011. Si j'estime qu'en fonction de certains facteurs des questions ou des activités sont prioritaires, elles pourraient être examinées plus rapidement. Cette situation fait partie du processus continu d'examen visant à recenser les secteurs où les risques d'atteinte à la loi ou à la vie privée sont les plus importants.

PLAINTES AU SUJET DES ACTIVITÉS DU CSTC

Mon mandat consiste notamment à entreprendre toute enquête que je juge nécessaire à la suite d'une plainte afin de déterminer si le CSTC a mené ou mène des activités illégales.

Cette année, mon bureau a reçu une plainte justifiant la tenue d'une enquête. Bien que je ne puisse commenter la teneur de la plainte, je suis en mesure d'affirmer que l'enquête a permis de conclure que le CSTC ne s'était livré à aucune activité illégale.

FONCTIONS EXERCÉES EN VERTU DE LA *LOI SUR LA PROTECTION DE L'INFORMATION*

La *Loi sur la protection de l'information* m'autorise à recevoir des renseignements de personnes astreintes au secret à perpétuité qui veulent se prévaloir de la défense « d'intérêt public » concernant la divulgation de renseignements classifiés relatifs au CSTC. Aucun problème de ce genre n'a été soumis à mon bureau pendant la période de référence 2008–2009.

LE BUREAU DU COMMISSAIRE

Au cours de 2008–2009, j'ai rencontré périodiquement le chef du CSTC pour discuter de questions d'intérêt mutuel. Ces rencontres de collaboration témoignent d'une relation de travail productive qui, selon moi, favorise l'efficacité et l'efficience générales du processus d'examen.

Au cours de la période de référence, j'ai eu l'occasion de rencontrer la conseillère à la sécurité nationale nouvellement nommée par le premier ministre, dont les responsabilités incluent celles relativement aux politiques et au fonctionnement du CSTC. J'ai également rencontré certains juges de la cour fédérale ainsi que d'autres hauts fonctionnaires.

Nouveau statut de mon bureau

Comme je l'ai mentionné dans mon dernier rapport, il a été décidé à l'automne 2007 de mettre fin à la relation de longue date que mon bureau entretenait avec le Bureau du Conseil privé et de confier au ministère de la Défense nationale les fonctions de soutien administratif et autres de mon bureau.

Par la suite, il a été établi que le positionnement de mon bureau au sein du même portefeuille que le CSTC semblait heurter les convenances et nuire à l'autonomie qui doit exister entre un organisme et son organe d'examen. Par conséquent, à compter du 1er avril 2009, mon bureau s'est vu accorder son propre crédit parlementaire. Bien que le lien hiérarchique avec le ministre de la Défense nationale demeure inchangé, comme le prévoit la *Loi sur la défense nationale*, mon bureau est un organisme distinct ne faisant pas partie de ce ministère.

Ces changements ont inévitablement donné lieu à une augmentation des dépenses relatives aux services de soutien, et à une augmentation correspondante du budget qui figure à l'annexe C. J'estime que ce nouveau statut est une autre preuve de l'évolution de mon bureau et du renforcement de son indépendance.

Conférence 2008 de l'Association canadienne pour les études de renseignement et de sécurité

Nous avons participé à la conférence annuelle de l'ACERS en octobre 2008, qui nous a donné une excellente occasion d'échanger sur les perspectives touchant les questions relatives à la sécurité et aux renseignements, y compris l'examen, avec des spécialistes, des chercheurs, des décideurs et des intervenants importants de partout au pays. Le personnel de mon bureau a beaucoup apprécié de guider deux étudiants canadiens diplômés en sécurité et renseignements dans le cadre de la conférence et des discussions.

Conférence internationale des organismes de surveillance du renseignement

En octobre 2008, dans le cadre de la Conférence internationale des organismes de surveillance du renseignement, à Auckland, en Nouvelle-Zélande, j'ai donné un exposé devant un groupe d'experts sur la façon d'établir un lien de confiance entre un organe d'examen et l'organisme soumis à l'examen, tout en conservant son indépendance. J'ai fait ressortir que l'établissement et le maintien du lien de confiance entre le CSTC et mon bureau, et la protection de l'indépendance de mon bureau, nécessitent une gestion constante des intérêts à tous les niveaux et des accommodements à cet égard.

J'ai également mis l'accent sur le fait que la confiance du CSTC à l'égard du Bureau du commissaire repose en grande partie sur la qualité évidente de ses examens. C'est pourquoi mon bureau attache une grande importance à l'élaboration, à la consignation et à la mise en œuvre de méthodes solides, reposant sur des normes acceptées en matière d'examen et plusieurs années d'expérience pratique. J'ai ajouté que mon bureau avait

mis au point des politiques et des procédures opérationnelles qui ont notamment permis d'orienter les employés dans l'exécution des examens, de garantir dans une large mesure la transparence et la cohérence du travail de mon équipe du point de vue du CSTC, et de servir de base à l'évaluation et à l'amélioration du rendement du CSTC pour la réalisation de son mandat.

British Intelligence and Security Committee of Parliamentarians

J'ai rencontré les membres du British Intelligence and Security Committee of Parliamentarians lors de leur visite à Ottawa en mars 2009. Les membres du comité, mon personnel et moi-même avons eu des échanges d'information et de points de vue utiles sur des questions d'intérêt et des préoccupations mutuelles touchant l'examen en matière de sécurité et de renseignements.

MOT DE LA FIN

En raison des réalisations actuelles, c'est avec satisfaction et optimisme dans l'avenir que je termine mon premier mandat à titre de commissaire du CST et que j'entreprends un deuxième mandat d'un an en août 2009. Au cours des trois dernières années, je suis heureux d'avoir établi une relation de travail productive avec le chef du CSTC. J'espère renforcer cette relation en continuant à examiner les activités de l'organisme conformément à mon mandat. Un examen exhaustif représente pour moi à la fois un défi et une tâche enrichissante que je suis fier d'accomplir au nom des Canadiens.

ANNEXE A : MANDAT DU COMMISSAIRE DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS

***Loi sur la défense nationale* – partie V.1**

273.63 (1) Le gouverneur en conseil peut nommer, à titre inamovible pour une période maximale de cinq ans, un juge à la retraite surnuméraire d'une juridiction supérieure qu'il charge de remplir les fonctions de commissaire du Centre de la sécurité des télécommunications.

(2) Le commissaire a pour mandat

a) de procéder à des examens concernant les activités du Centre pour en contrôler la légalité;

b) de faire les enquêtes qu'il estime nécessaires à la suite de plaintes qui lui sont présentées;

c) d'informer le ministre et le procureur général du Canada de tous les cas où, à son avis, le Centre pourrait ne pas avoir agi en conformité avec la loi.

(3) Le commissaire adresse au ministre, dans les quatre-vingt-dix jours suivant la fin de chaque exercice, un rapport sur l'exercice de ses activités. Le ministre dépose le rapport devant chacune des chambres du Parlement dans les quinze premiers jours de séance de celle-ci suivant sa réception.

(4) Dans l'exercice de son mandat, le commissaire a tous les pouvoirs conférés à un commissaire en vertu de la partie II de la *Loi sur les enquêtes*.

(5) Le commissaire peut retenir les services de conseillers juridiques ou techniques ou d'autres collaborateurs dont la compétence lui est utile dans l'exercice de ses fonctions; il peut fixer, avec l'approbation du Conseil du Trésor, leur rémunération et leurs frais.

(6) Le commissaire exerce les attributions que lui confèrent la présente partie et toute autre loi fédérale; il peut en outre se livrer à toute activité connexe autorisée par le gouverneur en conseil.

(7) La personne qui occupe, à l'entrée en vigueur du présent article, la charge de commissaire du Centre de la sécurité des télécommunications est maintenue en fonctions jusqu'à l'expiration de son mandat.

[...]

273.65 (8) Le commissaire du Centre de la sécurité des télécommunications est tenu de faire enquête sur les activités qui ont été exercées sous le régime d'une autorisation donnée en vertu du présent article pour en contrôler la conformité; il rend compte de ses enquêtes annuellement au ministre.

Loi sur la protection de l'information

15. (1) Nul ne peut être déclaré coupable d'une infraction prévue aux articles 13 ou 14 s'il établit qu'il a agi dans l'intérêt public. [...]

(5) Le juge ou le tribunal ne peut décider de la prépondérance des motifs d'intérêt public en faveur de la révélation que si la personne s'est conformée aux exigences suivantes : [...]

b) dans le cas où elle n'a pas reçu de réponse de l'administrateur général ou du sous-procureur général du Canada dans un délai raisonnable, elle a informé de la question, avec tous les renseignements à l'appui en sa possession : [...]

(ii) soit le commissaire du Centre de la sécurité des télécommunications si la question porte sur une infraction qui a été, est en train ou est sur le point d'être commise par un membre du Centre de la sécurité des télécommunications dans l'exercice effectif ou censé tel de ses fonctions pour le compte de celui-ci, et n'en a pas reçu de réponse dans un délai raisonnable.

ANNEXE B : RAPPORTS CLASSIFIÉS AU MINISTRE, 1996–2009

1. Principal vs. agent status – 3 mars 1997 (TRÈS SECRET)

2. Operational policies with lawfulness implications – 6 février 1998 (SECRET)

3. CSE's activities under *** – 5 mars 1998 (TRÈS SECRET Mot codé/Réservé aux Canadiens)

4. Internal investigations and complaints – 10 mars 1998 (SECRET)

5. CSE's activities under *** – 10 décembre 1998 (TRÈS SECRET/Réservé aux Canadiens)

6. On controlling communications security (COMSEC) material – 6 mai 1999 (TRÈS SECRET)

7. How we test (Rapport classifié sur la mise à l'essai des pratiques du CST en matière de collecte et de conservation de renseignements électromagnétiques, et évaluation des efforts de l'organisme pour sauvegarder la vie privée des Canadiens) – 14 juin 1999 (TRÈS SECRET Mot codé/Réservé aux Canadiens)

8. A study of the *** collection program – 19 novembre 1999 (TRÈS SECRET Mot codé/Réservé aux Canadiens)

9. On *** – 8 décembre 1999 (TRÈS SECRET/COMINT)

10. A study of CSE's *** reporting process — an overview (Phase I) – 8 décembre 1999 (SECRET/Réservé aux Canadiens)

11. A study of selection and *** — an overview – 10 mai 2000 (TRÈS SECRET/ Réservé aux Canadiens)

12. CSE's operational support activities under *** — follow-up – 10 mai 2000 (TRÈS SECRET/Réservé aux Canadiens)

13. Internal investigations and complaints — follow-up – 10 mai 2000 (SECRET)

14. On findings of an external review of CSE's ITS program – 15 juin 2000 (SECRET)

15. CSE's policy system review – 13 septembre 2000 (TRÈS SECRET/ Réservé aux Canadiens)

16. A study of the *** reporting process — *** (Phase II) – 6 avril 2001 (SECRET/Réservé aux Canadiens)

17. A study of the *** reporting process — *** (Phase III) – 6 avril 2001 (SECRET/Réservé aux Canadiens)

18. CSE's participation *** – 20 août 2001 (TRÈS SECRET/Réservé aux Canadiens)

19. CSE's support to ***, as authorized by *** and code-named *** – 20 août 2001 (TRÈS SECRET/Réservé aux Canadiens)

20. A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) – 21 août 2002 (SECRET)

21. CSE's support to ***, as authorized by *** and code-named *** – 13 novembre 2002 (TRÈS SECRET/Réservé aux Canadiens)

22. CSE's *** activities carried out under the *** 2002 *** Ministerial authorization – 27 novembre 2002 (TRÈS SECRET/Réservé aux Canadiens)

23. Lexicon of CSE definitions – 26 mars 2003 (TRÈS SECRET)

24. CSE's activities pursuant to *** Ministerial authorizations including *** – 20 mai 2003 (SECRET)

25. CSE's support to ***, as authorized by *** and code-named *** — Part I – 6 novembre 2003 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

26. CSE's support to ***, as authorized by *** and code-named *** — Part II – 15 mars 2004 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

27. A review of CSE's activities conducted under *** Ministerial authorization – 19 mars 2004 (SECRET/Réservé aux Canadiens)

28. Internal investigations and complaints — follow-up – 25 mars 2004 (TRÈS SECRET/Réservé aux Canadiens)

29. A review of CSE's activities conducted under 2002 *** Ministerial authorization – 19 avril 2004 (SECRET/Réservé aux Canadiens)

30. Review of CSE *** operations under Ministerial authorization – 1er juin 2004 (TRÈS SECRET/COMINT)

31. CSE's support to *** – 7 janvier 2005 (TRÈS SECRET/COMINT/ Réservé aux Canadiens)

32. External review of CSE's *** activities conducted under Ministerial authorization – 28 février 2005 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

33. A study of the *** collection program – 15 mars 2005 (TRÈS SECRET/COMINT/ Réservé aux Canadiens)

34. Report on the activities of CSE's *** – 22 juin 2005 (TRÈS SECRET)

35. Interim report on CSE's *** operations conducted under Ministerial authorization – 2 mars 2006 (TRÈS SECRET/COMINT)

36. External review of CSE *** activities conducted under Ministerial authorization – 29 mars 2006 (TRÈS SECRET/Réservé aux Canadiens)

37. Review of CSE'S foreign intelligence collection in support of the RCMP (Phase II) – 16 juin 2006 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

38. Review of information technology security activities at a government department under ministerial authorization – 18 décembre 2006 (TRÈS SECRET)

39. Review of CSE signals intelligence collection activities conducted under ministerial authorizations (Phase I) – 20 février 2007 (TRÈS SECRET/COMINT/ Réservé aux Canadiens)

40. Role of the CSE's client relations officers and the Operational Policy Section in the release of personal information – 31 mars 2007 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

41. Review of information technology security activities at a government department under ministerial authorization – 20 juillet 2007 (TRÈS SECRET)

42. Review of CSEC's counter-terrorism activities – 16 octobre 2007 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

43. Review of CSE's activities carried out under a ministerial directive – 9 janvier 2008 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

44. Review of CSEC's support to CSIS – 16 janvier 2008 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

45. Review of CSEC signals intelligence collection activities conducted under ministerial authorizations (Phase II) – 28 mars 2008 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

46. Review of CSEC's acquisition and implementation of technologies as a means to protect the privacy of Canadians – 11 juin 2008 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

47. Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 1) – 11 juin 2008 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

48. Review of disclosure of information about Canadians to Government of Canada clients – 19 novembre 2008 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

49. Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 2) – 13 janvier 2009 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

50. Review of CSEC foreign intelligence collection activities conducted under a ministerial directive and ministerial authorizations (Activity 3) – 26 février 2009 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

51. Review of CSEC activities conducted under a ministerial directive and in support of its foreign intelligence collection mandate – 12 mars 2009 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

52. Follow-up to a recommendation in a 2007–2008 review of CSEC activities carried out under a ministerial directive – 12 mars 2009 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

ANNEXE C : ÉTAT DES DÉPENSES, 2008-2009

Sommaire des articles courants

Traitements et salaires	782 686 $
Transports et télécommunications	43 337
Information	16 303
Services professionnels et spéciaux	258 294
Location	157 371
Achat de services de réparation et d'entretien	1 913
Fournitures et approvisionnements	7 822
Acquisition de machine et de matériel	23 595
Autres charges	0
Total	**1 291 321 $**

ANNEXE D : HISTORIQUE DU BUREAU DU COMMISSAIRE DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS (BCCST)

Le Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST) a été créé le 19 juin 1996, au moment de la nomination du premier commissaire, l'honorable Claude Bisson, O.C., ancien juge en chef du Québec. M. Bisson a occupé le poste de commissaire jusqu'en juin 2003. Le très honorable Antonio Lamer, c.p., C.C., c.d., L.L.D., d.u., ancien juge en chef du Canada (décédé), lui a alors succédé pour un mandat de trois ans. L'honorable Charles D. Gonthier, C.C., c.r., qui a pris sa retraite de la Cour suprême du Canada en 2003, a été nommé commissaire en août 2006.

Pendant les six premières années de son mandat (de juin 1996 à décembre 2001), le commissaire a exercé ses fonctions conformément à plusieurs décrets, pris en vertu de la partie II de la *Loi sur les enquêtes*. Au cours de cette période, il a assumé une double responsabilité : examiner les activités du Centre de la sécurité des télécommunications Canada (CSTC) afin de déterminer si elles étaient en conformité avec les lois du Canada, et recevoir les plaintes relatives aux activités du CSTC.

Dans le sillage des attentats terroristes du 11 septembre 2001, le Parlement a adopté la *Loi antiterroriste* omnibus, qui a été promulguée le 24 décembre 2001. Cette *Loi* modifie la *Loi sur la défense nationale*, en y ajoutant la partie V.1, qui établit le cadre législatif du BCCST et du CSTC, et elle confie au commissaire de nouvelles responsabilités relatives à l'examen des activités que mène le CSTC sous le régime d'une autorisation ministérielle.

En outre, la *Loi* omnibus a remplacé la *Loi sur les secrets officiels* par la *Loi sur la protection de l'information*, laquelle attribue au commissaire des fonctions précises pour les cas où une personne astreinte au secret à perpétuité souhaiterait invoquer la défense de l'intérêt public pour justifier la divulgation de renseignements classifiés sur le CSTC.

Il a été décidé à l'automne 2007 de mettre fin à la relation de longue date que le BCCST entretenait avec le Bureau du Conseil privé pour les fonctions de soutien administratif et autres du bureau. Le BCCST a reçu son propre crédit parlementaire le 1er avril 2009. Bien que le commissaire transmet toujours ses rapports au ministre de la Défence nationale, le BCCST est un organisme distinct, ne faisant pas partie de ce ministère.

ANNEXE E : RÔLE ET MANDAT DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS CANADA (CSTC)

Le Centre de la sécurité des télécommunications Canada (CSTC) est l'organisme national de cryptologie du Canada. Organisme unique en son genre au sein de la collectivité canadienne de la sécurité et du renseignement, le CSTC emploie des cryptologues pour protéger la sécurité des technologies de l'information du gouvernement du Canada et lui fournir des renseignements étrangers. Il offre en outre une assistance technique et opérationnelle aux organismes fédéraux chargés de la sécurité et de l'application de la loi.

Les produits et services de renseignement étranger du CSTC sont fournis à l'appui des décisions gouvernementales dans les domaines de la sécurité nationale, du renseignement national et de la politique étrangère. Ses activités en matière de renseignement électromagnétiques visent exclusivement des renseignements étrangers et sont assujetties aux priorités du gouvernement du Canada en matière de renseignement.

Dans le domaine de la sécurité des technologies de l'information, les produits et services du CSTC permettent à ses clients (les autres ministères et organismes gouvernementaux) d'assurer la sécurité de leurs systèmes et réseaux d'information électronique. Le CSTC effectue aussi des travaux de recherche-développement au nom du gouvernement du Canada dans des disciplines liées à la sécurité des télécommunications.

Le paragraphe 273.64(1) de la partie V.1 de la *Loi sur la défense nationale* établit le mandat du CSTC, qui comprend trois volets désignés sous le nom de parties a), b) et c) :

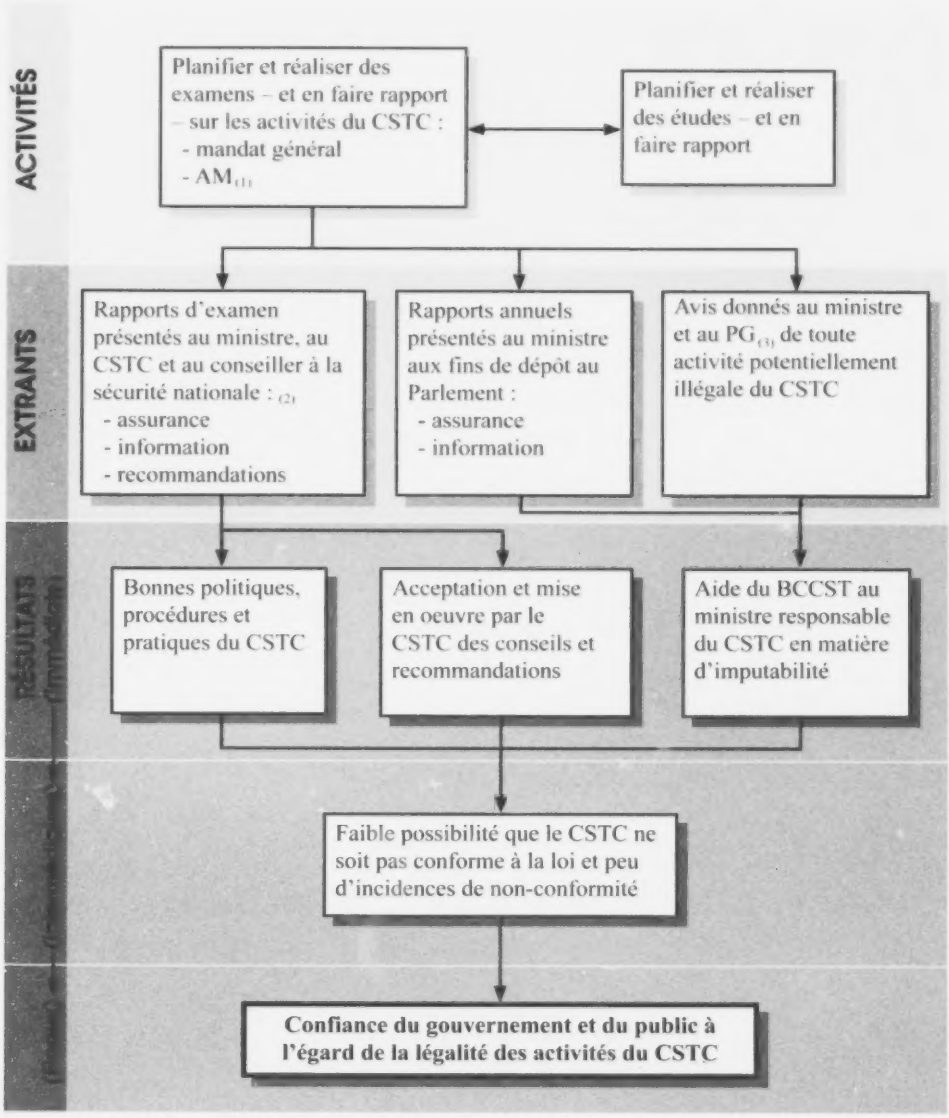
a) acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignement;

b) fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada;

c) fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité dans l'exercice des fonctions que la loi leur confère.

ANNEXE F : PROGRAMME D'EXAMEN DU BCCST — MODÈLE LOGIQUE

Le modèle logique suivant offre une description graphique de la façon dont le programme d'examen fonctionne.


ACTIVITÉS
Planifier et réaliser des examens – et en faire rapport – sur les activités du CSTC :
- mandat général
- AM(1)
Planifier et réaliser des études – et en faire rapport
EXTRANTS
Rapports d'examen présentés au ministre, au CSTC et au conseiller à la sécurité nationale : (2)
- assurance
- information
- recommandations
Rapports annuels présentés au ministre aux fins de dépôt au Parlement :
- assurance
- information
Avis donnés au ministre et au PG(3) de toute activité potentiellement illégale du CSTC
RÉSULTATS
Bonnes politiques, procédures et pratiques du CSTC
Acceptation et mise en oeuvre par le CSTC des conseils et recommandations
Aide du BCCST au ministre responsable du CSTC en matière d'imputabilité
Faible possibilité que le CSTC ne soit pas conforme à la loi et peu d'incidences de non-conformité
Confiance du gouvernement et du public à l'égard de la légalité des activités du CSTC

(1) Autorisations ministérielles (2) auprès du Premier ministre (3) Procureur général du Canada